Richtlinie zum „Software-Sprint“

MatrixConduit – Erweiterung und Stabilisierung des Conduit Matrix Servers mit einem Fokus auf Föderation

---

Schlussbericht

Zuwendungsempfänger:

Timo Kösters

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 01IS21S11 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Autor.

Kurze Darstellung der Aufgabenstellung und Motivation

Heutzutage benutzen viele Menschen Chat-Programme wie WhatsApp, Discord oder Microsoft Teams: Geschlossene Plattformen, von denen man abhängig ist und dessen Sicherheit man nicht überprüfen kann. MatrixConduit hilft dem Matrix Projekt, welches die Kontrolle über Chat-Nachrichten zurück in die Hände der Nutzer bringen will. So kann man sich zum Beispiel sicher sein, dass kein Dritter unbefugten Zugriff auf die Daten hat und durch Ende-zu-Ende Verschlüsselung ist zudem sichergestellt, dass selbst Besitzer von Servern nicht die Nachrichten von allen Nutzern auf diesem Server lesen können.

Geplante Meilensteine:
1. Vollständige Client-Server API Unterstützung: Alle möglichen Funktionen, die das Programm eines Endnutzers nutzen könnte sind möglichst vollständig implementiert.
2. Föderation mit anderen Servern: Damit wird ermöglicht, dass ein MatrixConduit Server mit jedem anderen Matrix Server zuverlässig kommunizieren und Daten austauschen kann.
3. App-Service Kompatibilität: App Services sind Programme, die über einen besonderen Weg mit einem Matrix Server sprechen können um Features wie z.B. Brücken in Netzwerke außerhalb von Matrix zu ermöglichen.
4. Optimierung: MatrixConduit benötigt wenige Resourcen und Daten werden effizient in der Datenbank abgelegt.
5. Administrierungs-Hilfen: Implementierung von Features, die das Administrieren, Moderieren und Steuern des Servers vereinfachen.
6. Migrations-Hilfen: Der Wechsel von dem offiziellen Matrix Server (Synapse) zu MatrixConduit soll leichter werden

Beitrag des Projektes zu den Zielen der Förderinitative „Software-Sprint“

MatrixConduit ist nun in der Beta-Phase und ermöglicht Einzelpersonen ohne große Kosten selber seine Chat-Daten privat zu speichern. Dabei steht vor allem der gesellschaftliche Nutzen im Vordergrund.

Nach Veröffentlichung der MatrixConduit Beta wurde die Webseite https://conduit.rs/release-0-2-0/ von über 12.000 unterschiedlichen Personen aufgerufen. Ein paar davon haben noch am selben Tag MatrixConduit heruntergeladen und auf ihrem eigenen Server ausprobiert.

Man kann zum Beispiel an dem Romeo and Juliet benchmark https://github.com/timokoesters/romeo-and-juliet-benchmark erkennen, dass Conduit Vorteile über Synapse und Dendrite bietet.

Ausführliche Darstellung der Ergebnisse

Meilenstein 1: Vollständige Client-Server API Unterstützung
- Lesebestätigungen über /receipt
- Push Nachrichten. Clients können Nachrichten empfangen ohne dass sie aktiv danach suchen
- Korrekte Generation von Vorschaubildern (Thumbnails) für Bilder
- Deutlich schnelleres Erkunden von Räumen
- Ende-zu-Ende Verschlüsselung

Meilenstein 2: Föderation mit anderen Servern
- State Resolution. Dies war das wichtigste Feature, da es die Sicherheit von Matrix ermöglicht
- Lücken in dem Nachrichtenverlauf werden erkannt und automatisch geschlossen
- Einladungen in Räume über Föderation
- Lesebestätigungen über Föderation
- Fehlgeschlagene Verbindungsversuche werden wiederholt

Meilenstein 3: App-Service Kompatibilität
Dank diesem Meilenstein ist es nun möglich einen MatrixConduit Server als Brücke in viele andere Netzwerke zu verwenden. Getestet wurden zum Beispiel Discord, Telegram und Hangouts.

Meilenstein 4: Optimierung
- Support für Jaeger um Performance Probleme zu analysieren
- Deutlich bessere /sync Performance, indem effizienter berechnet und gespeichert wird, was der Client wissen muss
- Neu entwickelter Algorithmus der den Zustand eines Raumes in einer sehr effizienten Form mit Hilfe von Differenzen zu anderen Zuständen speichert
- Sehr viele Caches für alle möglichen Operationen

Meilenstein 5: Administrierungs-Hilfen
Es wurden mehrere Dokumente geschrieben, die das Aufsetzen und Upgraden der Conduit Installation, sowie das Verbinden mit App-Services erklären, jedoch konnten Moderations-Hilfen aus zeitlichen Gründen noch nicht programmiert werden.

Meilenstein 6: Migrations-Hilfen
Dieses Ziel konnte leider nicht umgesetzt werden da es einen grösseren Umfang als erwartet hat und nicht mehr viel Zeit blieb. Jedoch war es als letzter Meilenstein auch nur als Bonus gedacht und ist für die Nutzung von Conduit nicht notwendig sondern lediglich eine Erleichterung für Personen die schon einen anderen Server haben, aber auf Conduit umsteigen möchten.

Zielgruppe, Nutzen und mögliche Weiterentwicklungen

MatrixConduit kann auf günstigen Servern installiert werden und erlaubt es Einzelpersonen, unabhängig von großen Unternehmen, Nachrichten sicher an andere teilen zu können.

Ich konnte über 500 Personen überzeugen den offiziellen #conduit Chat-Raum auf Matrix beizutreten, wo Fragen gestellt werden und auch über die Entwicklung von Conduit diskutiert wird. Mir haben über 40 Personen bei der Entwicklung von Conduit geholfen indem sie Code oder Dokumentation beigetragen haben. Die Pläne für die Zukunft sind die fehlenden Meilensteine und weitere Verbesserungen die MatrixConduit zu einem besseren Projekt machen. Außerdem ist es möglich, dass Conduit für Experimente genutzt wird, die dem gesamte Matrix Projekt helfen. Ich konnte viel über die Arbeit an Open-Source Projekten lernen.

Die nächsten Ziele sind folgende:

- Datenbank Optimierungen, sodass weniger IO notwendig ist und weniger RAM gebraucht wird.
- Nutzer Verifikation der Schlüssel bei der Ende-zu-Ende Verschlüsselung ist momentan nur lokal möglich, für Föderation müssen jedoch noch Endpunkte implementiert werden.
- Das Laden von Chat Nachrichten von bevor man einen Raum betreten hat.

Kurze Angabe von Präsentationsmöglichkeiten für mögliche Nutzer

Aktuelle Informationen zum Projekt sind auf https://conduit.rs

Kurze Erläuterung zur Einhaltung der Arbeits- und Kostenplanung

Die Optimierung der RAM- und Festplattennutzung hat deutlich mehr Zeit in Anspruch genommen als im vorhinein absehbar war, deshalb konnten die letzteren Meilensteine nicht erreicht werden. Ein Grund dafür war, dass wir von sled auf sqlite umsteigen mussten, da sled zu viel RAM benötigte und nicht wieder freigegeben hat.

Kurze Darstellung von etwaigen Ergebnissen bei anderen Stellen

Meine Arbeit war auch mit vielen kleinen Verbesserungen an anderen Open-Source Projekten verbunden. Zum Beispiel bei diesen Projekten:

- https://github.com/matrix-org/matrix-doc: Matrix Spezifikation
- https://github.com/matrix-org/matrix-ios-sdk: Matrix iOS SDK
- https://github.com/matrix-org/matrix-js-sdk: Matrix Javascript SDK
- https://github.com/matrix-org/matrix-react-sdk: SDK für Browser Matrix Client
- https://github.com/vector-im/element-android: Matrix Client für Android
- https://github.com/ruma/ruma: Matrix Bibliothek für Rust