Verteilte Systeme im Sommersemester 2023

Luca Schöneberg, Matr. Nr. 979049
Henry Wulff, Matr. Nr. 1014530 Osnabrück, 25.04.2023

Aufgabenblatt 4 - Publish-Subscribe-System mit RPCs

Beantworten Sie im Protokoll darüber hinaus die folgenden Fragen:

1. **Receiver und Client sind voneinander getrennte Prozesse. Warum ist dies so?**

   Receiver und Client sind voneinander getrennte Prozesse, um eine klare Trennung der Verantwortlichkeiten und eine bessere Skalierbarkeit zu ermöglichen. Der Receiver ist dafür zuständig, die vom Dispatcher gesendeten Nachrichten zu empfangen und auf der Konsole auszugeben.

   Der Client hingegen steuert den Nachrichtenempfang, indem er den Receiver beim Dispatcher registriert und deregistriert und die Nachrichten-Topics setzt. Durch diese Trennung können mehrere Clients und Receiver unabhängig voneinander arbeiten, und das System kann leichter erweitert werden.

2. **Handelt es sich um ein synchron oder asynchron arbeitendes System? Woran machen Sie das fest?**

   Das System arbeitet asynchron, da Nachrichten von Publishern an den Dispatcher gesendet werden, der sie dann an die entsprechenden Subscriber weiterleitet. Dabei werden Nachrichten über die gRPC-Schnittstelle übermittelt, die auf dem asynchronen Transport von Nachrichten basiert.

   Die Asynchronität zeigt sich darin, dass Publisher Nachrichten senden können, ohne auf eine direkte Antwort der Empfänger zu warten, und Empfänger Nachrichten empfangen und verarbeiten können, ohne den Sender direkt zu beeinflussen.

3. **Die Registrierung / De-Registrierung erfolgt über IP-Adressen. gRPC arbeitet mit http als Transport-Protokoll und kann auch zum Aufrufen von Diensten im Internet (evtl. Cloud) genutzt werden. Welche Probleme können dabei auftreten?**

   Bei der Verwendung von IP-Adressen zur Registrierung und De-Registrierung von Empfängern können verschiedene Probleme auftreten, insbesondere wenn gRPC über das Internet oder in Cloud-Umgebungen verwendet wird:

   a. IP-Adressen können sich ändern, z.B. durch dynamische IP-Vergabe von Internet-Service-Providern oder innerhalb von Cloud-Umgebungen. Dies kann dazu führen, dass ein Client plötzlich nicht mehr erreichbar ist oder Nachrichten an die falsche Adresse geschickt werden.
   b. IP-Adressen allein sind möglicherweise nicht ausreichend, um Clients eindeutig zu identifizieren, insbesondere in Umgebungen mit Network Address Translation (NAT), wenn mehrere Clients hinter der gleichen öffentlichen IP-Adresse agieren.
   c. Die Verwendung von IP-Adressen als Identifikator kann zu Sicherheitsproblemen führen, da Angreifer potenziell die IP-Adressen von legitimen Clients fälschen und so unerwünschten Zugriff auf Nachrichten erhalten könne.

   Um diese Probleme zu lösen, könnte man beispielsweise ein Authentifizierungs- und Autorisierungssystem implementieren, das auf Client-Identifikatoren und Zugriffstokens basiert, anstatt sich ausschließlich auf IP-Adressen zu verlassen.