

Untersuchung der Maßnahmen zur Gewährleistung von Sicherheit bei Nutzung einer Redpanda Message Queue



Meryem Kilic, Trainee MATSE

Motivation

- CANCOM bietet Kunden virtuellen Arbeitsplatz an (FIM-Portal)
- Aktuell: verteilter Monolith
- Plan für die Zukunft: Umstieg auf Message Queue
- Ziel dieser Arbeit: Analyse von benötigten Sicherheitsmaßnahmen



Inhalt

1. Message Queuing Technologie:

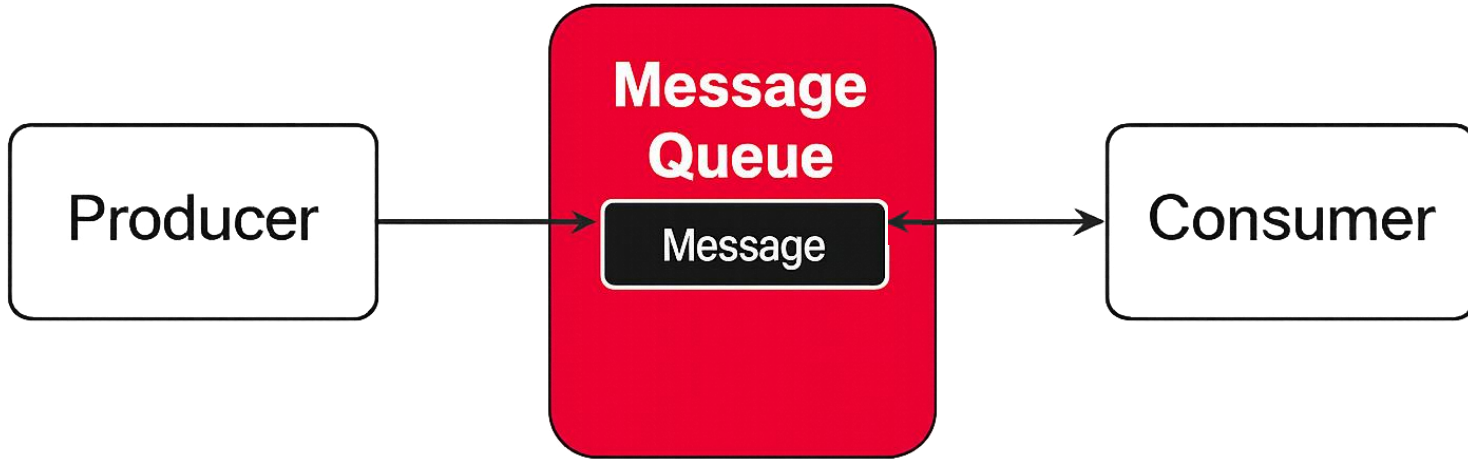
- Message Queuing: Grundlagen
- Eingesetzte Technologie: Redpanda

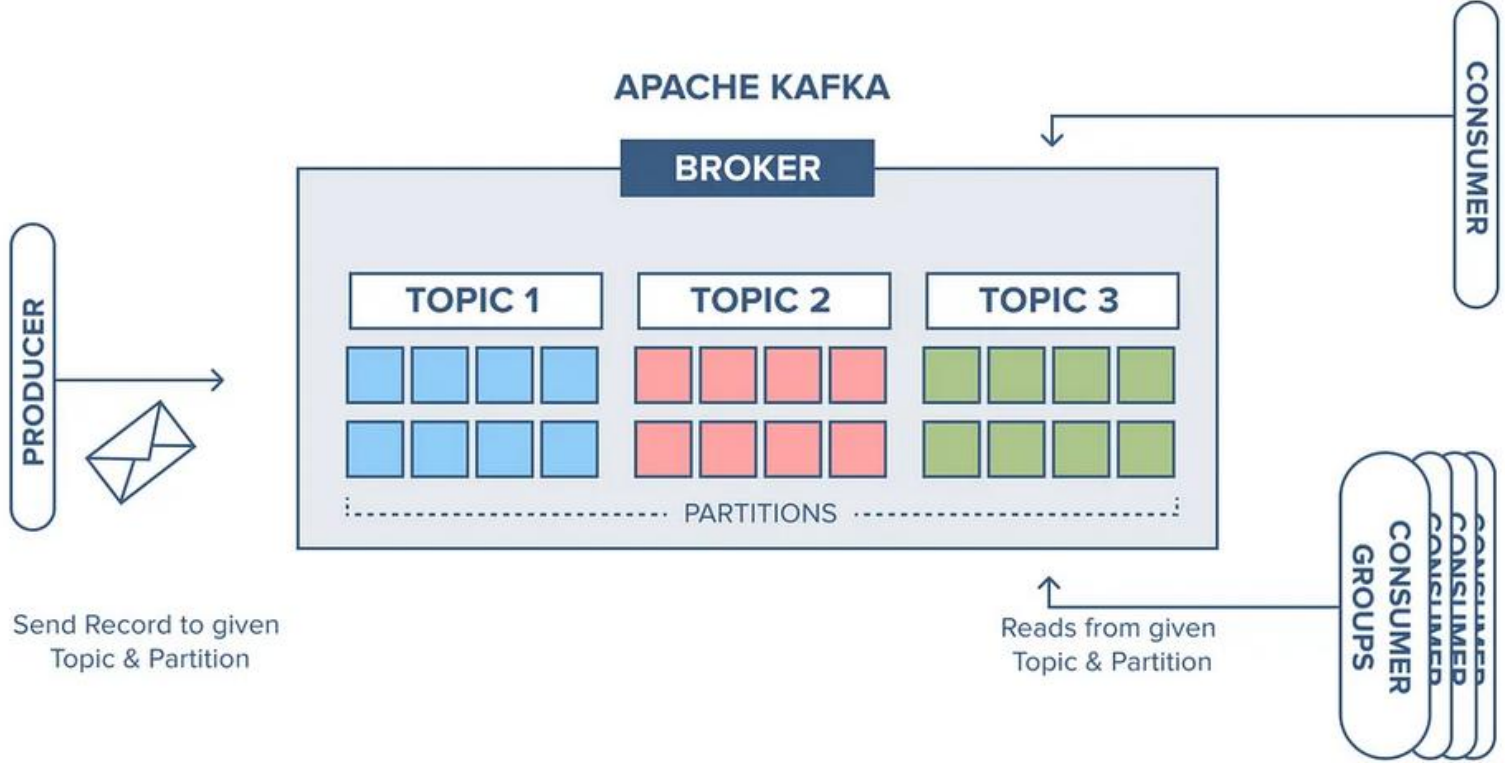
2. Sicherheitsanalyse:

- OWASP Top Ten 2021
- Auswahl an Sicherheitsmaßnahmen

Technologie

Message Queuing System





Eingesetzte Technologie: Redpanda

- Kafka-kompatible Streaming-Datenplattform (gleiche APIs)
- Besteht ähnlich wie Kafka aus Topics und Partitionen
- Leichtgewichtiger
- Alle Komponenten (Broker, Koordination) integriert



Redpanda

Sicherheitsanalyse

Open Worldwide Application Security Project Foundation (OWASP)

- Gemeinnützige Organisation
- Setzt sich für die Verbesserung von Sicherheit bei Software ein (Workshops, Konferenzen, ...)
- OWASP Top 10



OWASP Top 10 2021

1. Broken Access Control
2. Cryptographic Failures
3. Injection
4. Insecure Design
5. Security Misconfiguration
6. Vulnerable and Outdated Components
7. Identification and Authentication Failures
8. Software and Data Integrity Failures
9. Security Logging and Monitoring Failures
10. Server-Side Request Forgery (SSRF)

OWASP Top 10 2021

1. Broken Access Control
2. Cryptographic Failures
3. Injection
4. Insecure Design
5. Security Misconfiguration
6. Vulnerable and Outdated Components
7. Identification and Authentication Failures
8. Software and Data Integrity Failures
9. Security Logging and Monitoring Failures
10. Server-Side Request Forgery (SSRF)

Broken Access Control

Probleme in der Zugriffsrechteverteilung



Lösung: Acces Control Lists (ACL)

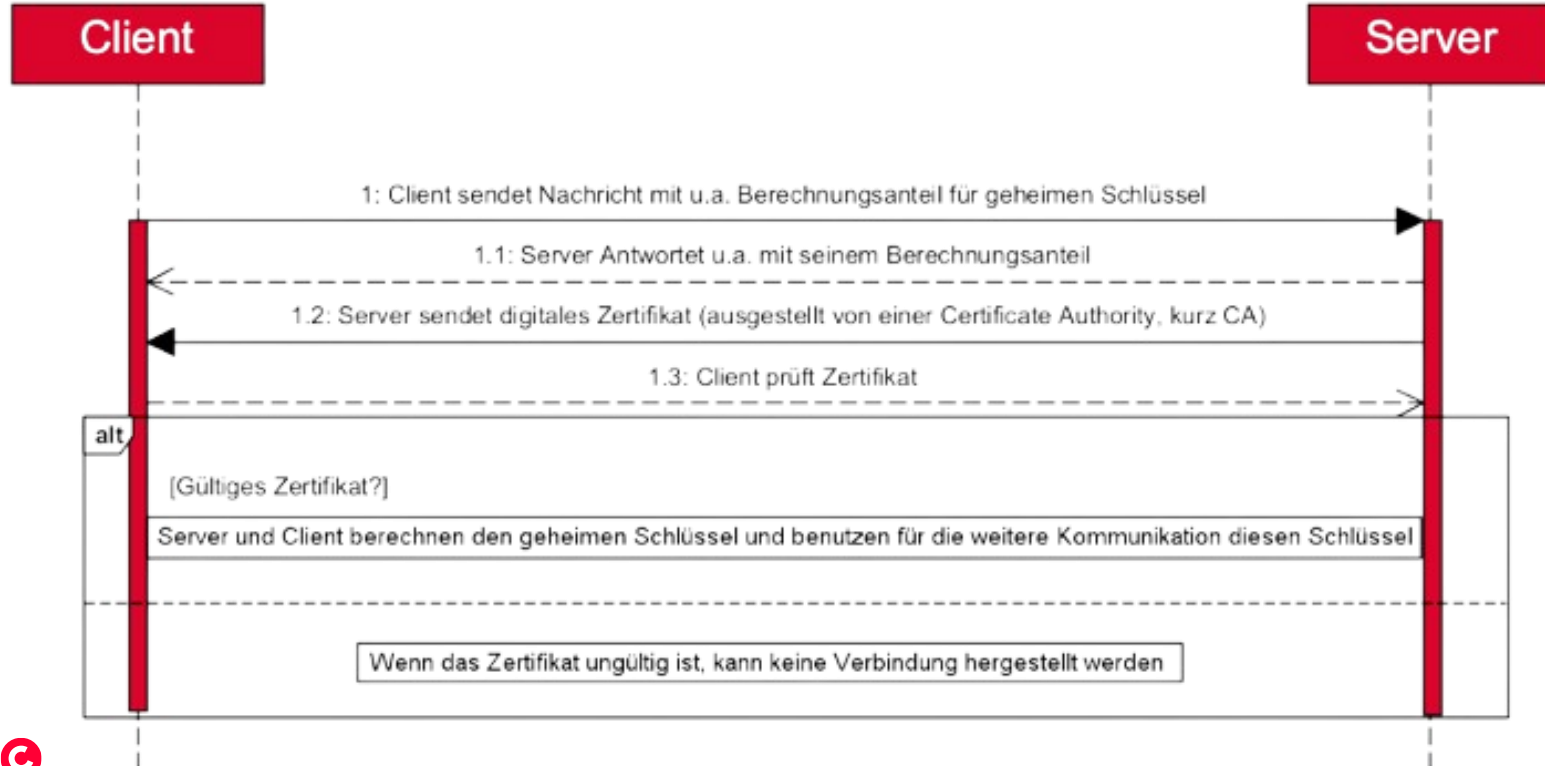
```
resource "kafka_acl" "example" {  
  resource_name      = kafka_topic.example.name  
  resource_type      = "Topic"  
  acl_principal      = "User:user01" # Replace with your principal  
  acl_host           = "*"   
  acl_operation       = "Write"  
  acl_permission_type = "Allow"  
}
```

Cryptographic Failures

Sicherheitslücken, die unzureichende Verschlüsselung betreffen



TLS-Verschlüsselung



Cryptographic Failures

- Im FIM-Team wird aufgrund fehlender CA aktuell keine TLS-Verschlüsselung genutzt
- Empfehlung: Nach Migration auf Kubernetes (Tool zum Verwalten containerisierter Anwendungen) einrichten

Insecure Design

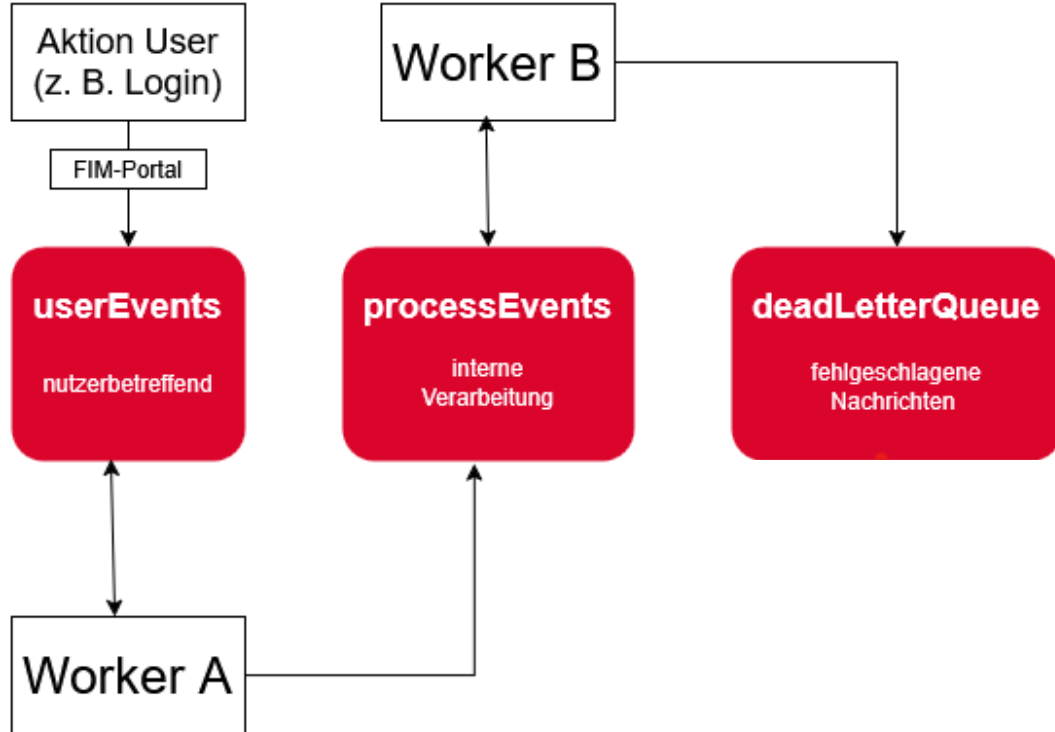
Entscheidungen in der Entwurfsphase, die Sicherheitslücken hervorbringen



Secure by Design

„Sicherheit [muss] bereits Bestandteil der Planungsphase sein. Idealerweise sollte [...] die Software so entworfen werden, dass Sicherheitsaspekte integrale Bestandteile der System- und Softwarearchitektur darstellen.“

Design des Message Queuing Systems



Kritische Worker: audit und dlq

- **audit:** speichert Nachrichten zu Analyse- und Nachvollziehbarkeitszwecken
 - **dlq:** liest die Dead Letter Queue aus
- ⇒ Beide Worker haben Zugriff auf eine große Bandbreite an Daten

Identification and Authentication Failures

Gefahren, die dadurch entstehen, dass User nicht eindeutig identifizierbar sind



SASL

- Jeder Worker besitzt einen User, mit dem er anmeldet, um auf die Queue zuzugreifen
- Login erfolgt über Simple Authentication and Security Layer (SASL), Clients werden über verschlüsselten Mechanismus identifiziert
- Passwörter der Worker werden verschlüsselt übertragen (klare Identifizierbarkeit)

Security Logging and Monitoring Failures

Das Nichterfassen sicherheitsrelevanter Aktivitäten





Ausblick

- Regelmäßige Sicherheitskontrollen sind unerlässlich
 - OWASP Top Ten 2025 hat neue Platzierungen
 - LLMs, KI

Quellen

https://docs.google.com/document/d/1o6Z2zwJn-cdNKWYz1V35_P8V6G_kFJyAVi561nUMep0/view?usp=sharing

