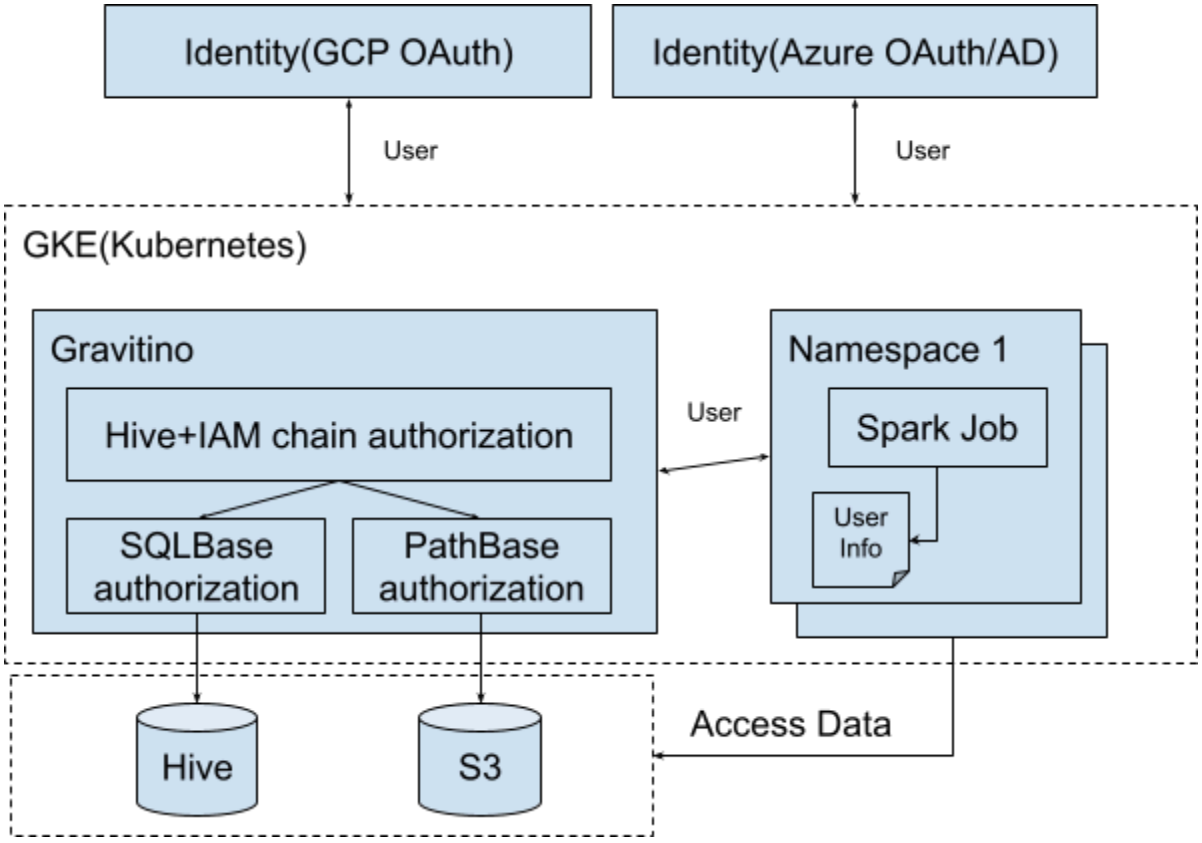
Gravitino access control 0.8

Key Point Requirements

1. Supports GCP OAuth or Azure OAuth/AD identity.
2. Synchronous authorization Hive and S3 IAM.
3. Set different execution users in different Spark jobs in the Kubernetes namespaces
4. Unified identity authentication for Gravitino, Kubernetes, Spark, and IAM is required

Solution



1. Supports GKE E2E scenario.
    a. Enables GCP OAuth (or Azure OAuht/AD)
        i. Gravitino enables OAuth
        ii. Spark executes user Identity authentication
    b. Deploying Gravitino, Spark on GKE
    c. Use Gravitino to unified authorization Hive and S3 IAM permission

d. Use different execution users in different Spark jobs in the Kubernetes namespaces

Reference

1. SQL Based Authorization Plugin
2. The Support Of Relational Chained Authorization Plugin
3. Gravitino access control 0.8