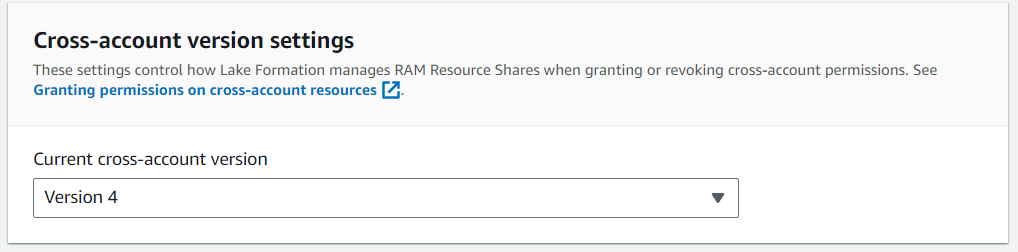
CROSS-ACCOUNT SHARING USING AWS LAKE FORMATION

To demonstrate the Lake Formation cross-account data sharing in Version 4.



**Prerequisites**

You need the following prerequisites:

* Two AWS accounts.
* An admin IAM user in both accounts.
* Lake Formation mode enabled in both the producer and consumer account with cross-account Version 4.

**Infra State:**

1. **An AWS account for managing all the access. Let us call it Central Account.**

This account has below IAM users:

* **lf-admin**: Have Administrator Access. Manages the data lake of all the other accounts. Manages all the user permission entitlements.

**Note:**

The purpose of this account is to register S3 Data location from other AWS accounts and create Glue Data Catalog over it. Moreover, when Glue Data Catalogs are created, permissions on these Glue Catalogs are supposed to be provided to cross account IAM principals to access in desired manner.

1. **An AWS account to which the data catalogue to be shared. Let’s call it Domain Account.**

This account has below IAM users:

* 1. **lf-analyst**: The analysts in the team needs access to data catalog.

**Note:** The purpose of this account is to only hold the data in S3 buckets.

## Setup Steps in Risk Account

## S3 Bucket and Data Setup

## Create a bucket name risk-transactions.

## Add two child folders to the bucket named executions-data and quotations-data.

## Add JSON data files to each folders.

## 

## 

## Setup Steps in Central Account

## AWS OU setup

## Navigate to AWS Organizations.

## Create a new Organizational Unit named SAP-UNIT.

## Add AWS accounts in this newly created Organizational Unit.

## Note: The accounts could also exist in different Organizational Unit for this demo to work.

## 

## Enable Sharing with AWS Organizations.

## Navigate to AWS Resource Access Manager.

## Enable sharing with AWS Organizations and Save Settings.

## 

## Create Glue Data Catalog

## Navigate to AWS Glue 🡪 Databases.

## Create database: risk\_transactions\_db

## Add table to created database.

## 

## 

## Verify Glue Data Catalog accessible in Lake Formation

## Verify that above created Glue Catalog (databases and tables) are visible in Lake Formation.

## 

## Grant Data Lake permissions to Cross Account.

## Grant permissions on Databases.

## Navigate to AWS Lake Formation.

## Go to Databases.

## Select Database

## Click on Actions 🡪 Grant

## In Principals section:

## Select External Account (permission is to be shared with i.e. lf-analyst)

## Choose IAM user/roles/principal

## In LF Tags/Catalog Resources section:

## Select Named Data Catalog Resources.

## Select database.

## In Database permissions section:

## Add Describe Permissions

## Grant the permission.

## Grant permissions on Database Tables.

## Navigate to AWS Lake Formation.

## Go to Tables.

## Select Table 🡪 quotations.

## Click on Actions 🡪 Grant

## In Principals section:

## Select External Account (permission is to be shared with i.e. lf-analyst)

## Choose IAM user/roles/principal

## In LF Tags/Catalog Resources section:

## Select Named Data Catalog Resources.

## Select database.

## Select tables.

## In Table permissions section:

## Add Select Describe Permissions

## Grant the permission.

## 