Hi Sandip

Please find below the updates on the implementation of row level data filter permission creation and sharing.

The complete implementation of this requirement was divided into following subtasks:

|  |  |  |
| --- | --- | --- |
| **Tasks** | **Change Details** | **Status** |
| Read the filter expression from the existing CSV file (which is being used to create database/table permissions) | Started reading the column filter\_expression validating the header from the incoming csv. | Done |
| Syntactic validation of the filter expression | Built an annotation driven API to validate the filter expression syntactically using ANTLR for partiql using partiql grammar | Done |
| Semantic validation of the filter expression | Built an API to validate the filter expression semantically using sqlparse library which can convert any partiql expression into a normalized expression. | Done |
| Validation on existence of data filter in dymanodb | Built a validation utility function to check if data filter already exists, if belongs redundantly to a unique partition key of accountId|databaseName|TableName | Done |
| API to grant data filter permissions and persist the newly created data filter name & expression in dynamodb | Built a utility class implementing the read and write operation for aws service (especially dynamodb & lakeformation) for creation of data filter permission and data read & write to dynamodb | Done |

While I have implemented all these changes above, I also tried finding a way for cross account resource sharing of Data filters, which could have worked in a way that we get to create the data filters in central account only and eventually share those data filters with the help of AWS organizations management and AWS RAM services, such that domain account can create permissions by managing the data filter themselves.

But unfortunately, the way AWS provides mechanisms to cross-account resource share of Data Catalogs (Databases/tables), it doesn't provide any similar mechanism to share Data Filters. The data filters always need to be created in the respective domain accounts to manage the data filter permissions. And this does not seem to be a scalable approach.

***References:***

https://docs.aws.amazon.com/ram/latest/userguide/shareable.html#shareable-glue

https://docs.aws.amazon.com/lake-formation/latest/dg/cross-account-named-resource.html