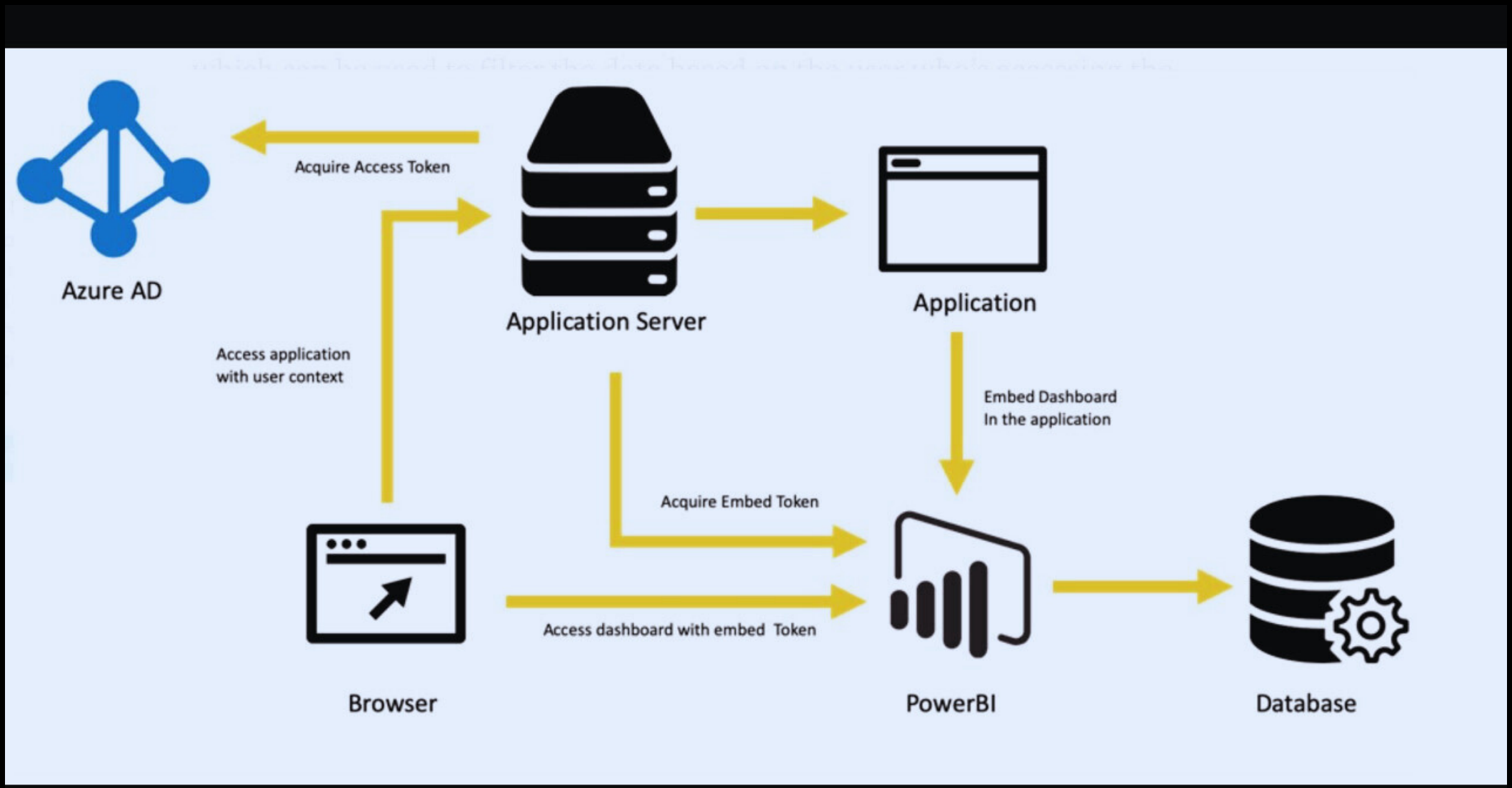
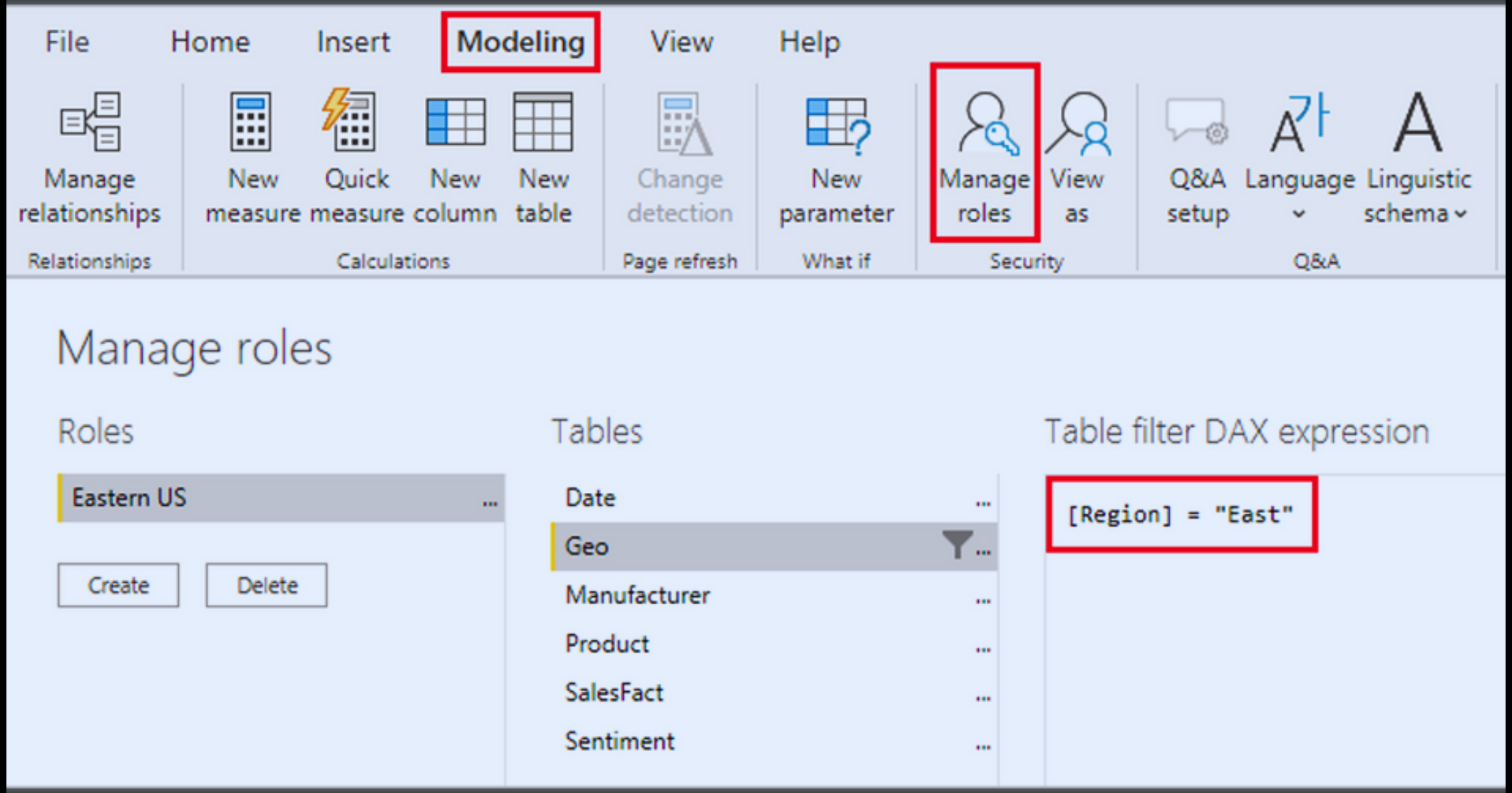
DATA SECURITY: ROW LEVEL SECURITY(RLS)

Archana Balasubramanian

ROW-LEVEL SECURITY (RLS)

- RLS restricts access to data at the row level based on defined criteria.
- It ensures users only see authorized data, enforcing security policies and protecting sensitive information.

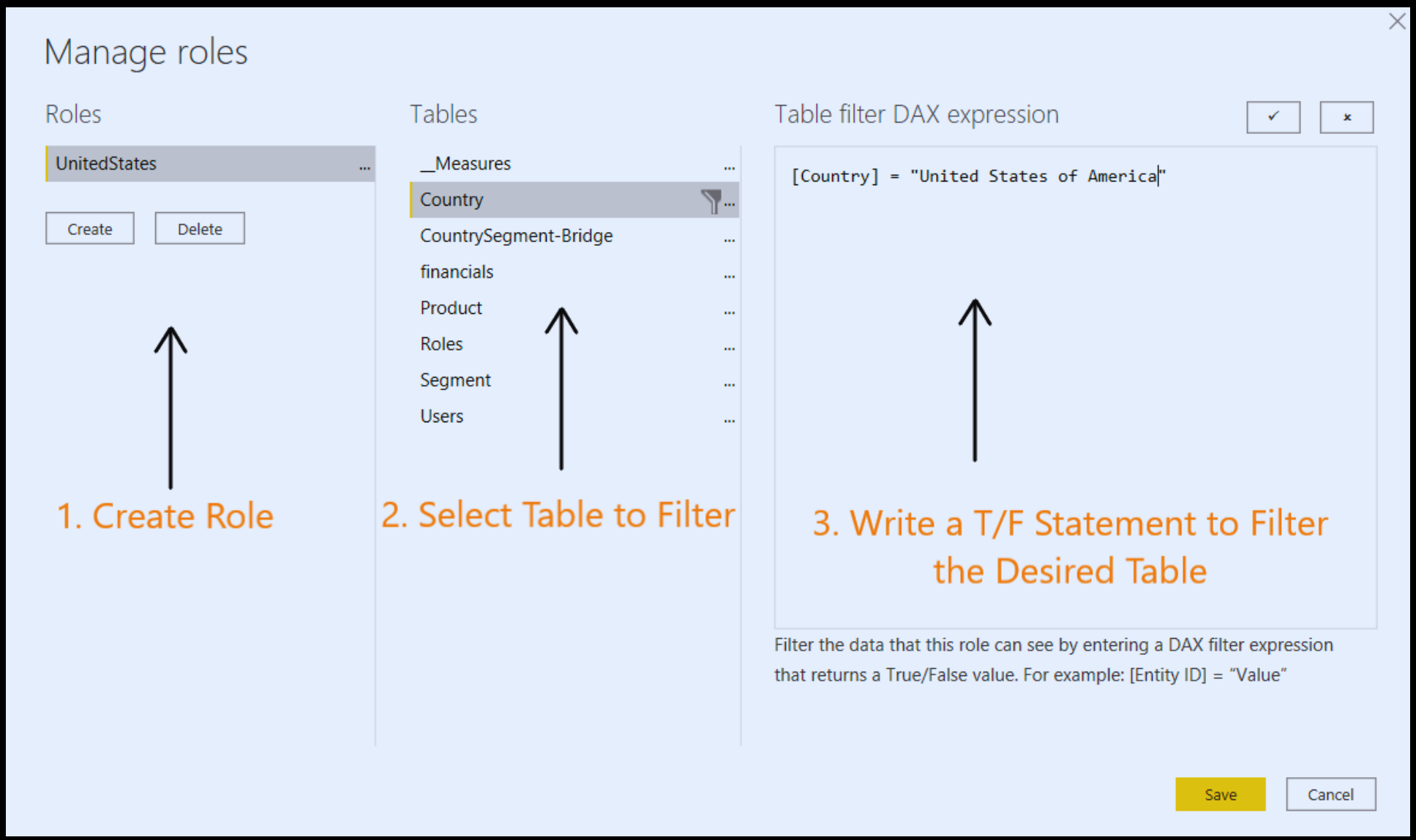

Azure AD
Acquire Access Token
Application Server
Application
Access application
with user context
Embed Dashboard
In the application
Acquire Embed Token
Access dashboard with embed Token
Browser
PowerBI
Database


File
Home
Insert
Modeling
View
Help
Manage relationships
Relationships
New measure
Quick measure
New column
New table
Calculations
Change detection
Page refresh
New parameter
What if
Manage roles
View as
Security
Q&A setup
Language
Linguistic schema
Q&A
Manage roles
Roles
Eastern US
Create
Delete
Tables
Date
Geo
Manufacturer
Product
SalesFact
Sentiment
Table filter DAX expression
[Region] = "East"

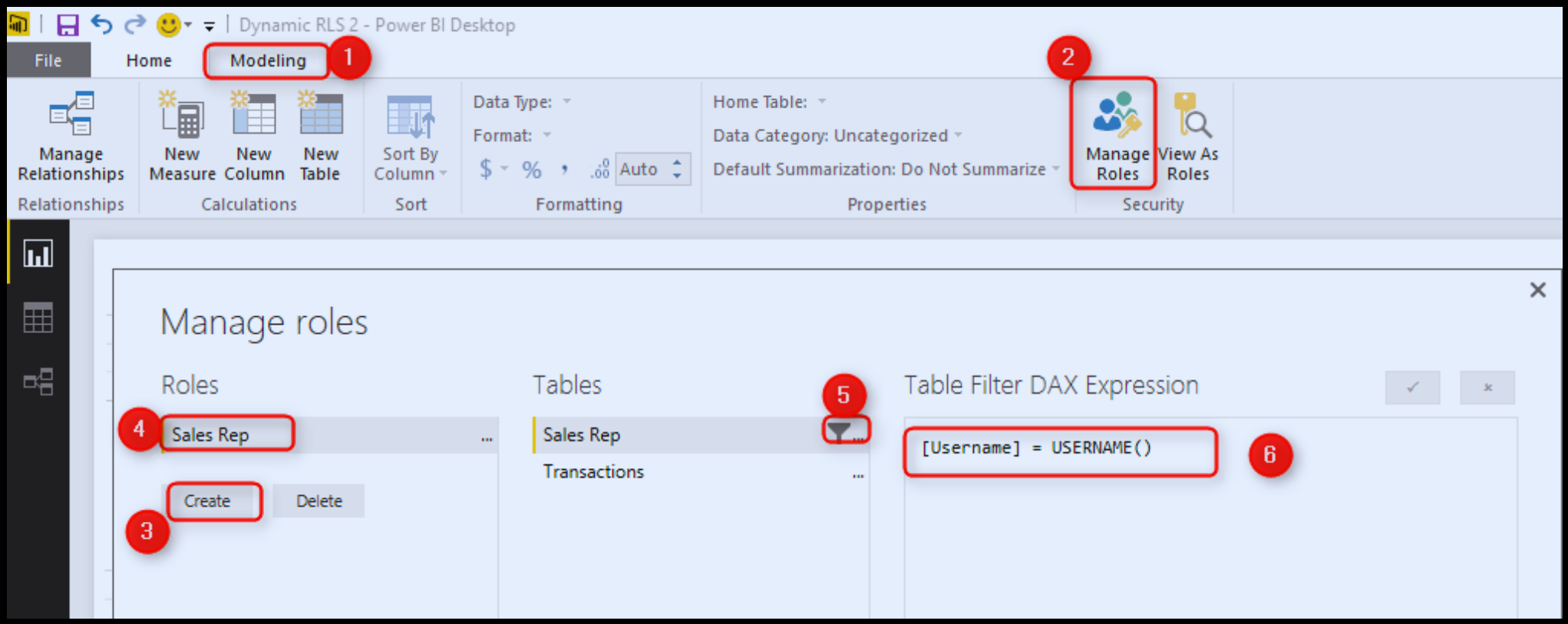
TYPES OF ROW-LEVEL SECURITY

- Static RLS: Filters based on fixed criteria.
- Dynamic RLS: Filters based on dynamic criteria like user identity.

STATIC RLS


Manage roles
Roles
UnitedStates
Create
Delete
Tables
__Measures
Country
CountrySegment-Bridge
financials
Product
Roles
Segment
Users
Table filter DAX expression
[Country] = "United States of America"
1. Create Role
2. Select Table to Filter
3. Write a T/F Statement to Filter the Desired Table
Filter the data that this role can see by entering a DAX filter expression that returns a True/False value. For example: [Entity ID] = "Value"
Save
Cancel

DYNAMIC RLS


Dynamic RLS 2 - Power BI Desktop
File
Home
Modeling
1
2
Manage Relationships
New Measure
New Column
New Table
Sort By Column
Data Type:
Format:
Auto
Home Table:
Data Category: Uncategorized
Default Summarization: Do Not Summarize
Manage Roles
View As Roles
Relationships
Calculations
Sort
Formatting
Properties
Security
Manage roles
Roles
Tables
Table Filter DAX Expression
4
Sales Rep
Create
Delete
3
Sales Rep
Transactions
5
[Username] = USERNAME()
6

DIFFERENCE BETWEEN STATIC AND DYNAMIC ROW-LEVEL SECURITY

- Static RLS uses fixed criteria, while dynamic RLS adapts based on user attributes or context.

ROLES AND ROLE-BASED FILTERS

- Roles are defined in Power BI Desktop or the Power BI Service. You can define roles based on user attributes or job functions.

- Role-based filters are created using DAX expressions to specify which rows of data users in each role can access. These filters are applied to tables in the data model.

SECURITY FILTERS

- Security filters are DAX expressions restricting data access.
- In RLS, they define which rows users in each role can access.

PROCESS OF ASSIGNING USERS TO ROLES

- Users are assigned to roles in Power BI Desktop or the Power BI Service.
- Role assignments are managed through the Power BI Service, where users are added to roles and removed as needed.

BEST PRACTICES FOR IMPLEMENTING RLS

- Regularly review and update RLS rules.
- Thoroughly test RLS to ensure correct data access.
- Use dynamic RLS for flexibility.

REPORT PERFORMANCE

- RLS can impact performance, especially for large datasets.
- Optimize by monitoring query execution and refining DAX expressions and data model design.

DATA PRIVACY AND COMPLIANCE

- RLS can impact performance, especially for large datasets.
- Optimize by monitoring query execution and refining DAX expressions and data model design.

TEST AND VALIDATION PROCESS

- Use test accounts representing different user roles.
- Utilize Power BI's View as Role feature to simulate user roles.

SAVE THIS POST IF YOU FIND IT USEFUL

Archana Balasubramanian