Understanding the basics of RLS

Row-Level Security (RLS)

Row-Level Security (RLS) in Power BI allows you to **restrict data access for specific users** based on roles. It ensures that users only see the data that is relevant to them, protecting sensitive information and ensuring data privacy.

Define RLS

RLS enables organizations to control access to data at a **row level**. It works by filtering rows of data based on the **user's role** or credentials. This can be useful in scenarios where different departments or individuals should only access data relevant to their role (e.g., sales data by region or department-specific data).

Types of RLS

1. **Static RLS**
    - Static RLS assigns specific row-level permissions **manually**. It applies a **predefined filter** for users based on their roles.
    - Example: A sales team only sees data for their assigned region, and this doesn't change dynamically based on who is logged in.
2. **Dynamic RLS**
    - Dynamic RLS **automatically adjusts** the data visible to each user based on their credentials (e.g., their username or email). The filtering criteria are based on user attributes stored in a table.
    - Example: A user logs in, and based on their username or group membership, the system filters data specific to them.
