SUPERSTORE ANALYSIS

VACANT

Presented by Group 6

AGENDA

1 External Stage

2 Scheduler

3 Auto Ingestion of Data
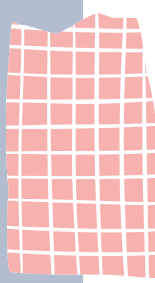
4 Slowly Changing Dimension

5 Column Level Masking

6 Row Level Security

1. WHAT IS EXTERNAL STAGE?

- Store the files in an external location (S3 bucket) that is referenced by the stage.

- It specifies integration object, location and credential information for the S3 bucket.
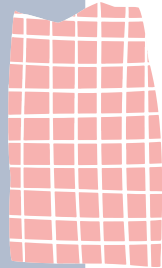
EXTERNAL STAGE IMPLEMENTATION

1. Integration object creation
2. Description of Integration object
3. Creating External stage
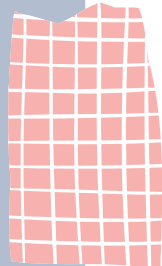4. Loading the data from the External Stage to the respective Table

2. WHAT IS SCHEDULER?

- **It is a process to execute a set of instructions in a defined time.**

- **Tasks can run according to a set interval and/or a flexible schedule using a subset of cron utility syntax.**
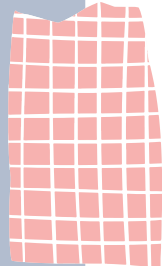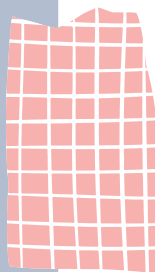
SCHEDULER IMPLEMENTATION

1. Created a task to schedule a job at 12:00 AM IST hours every Thursday
2. The task will load the data from external stage to source table
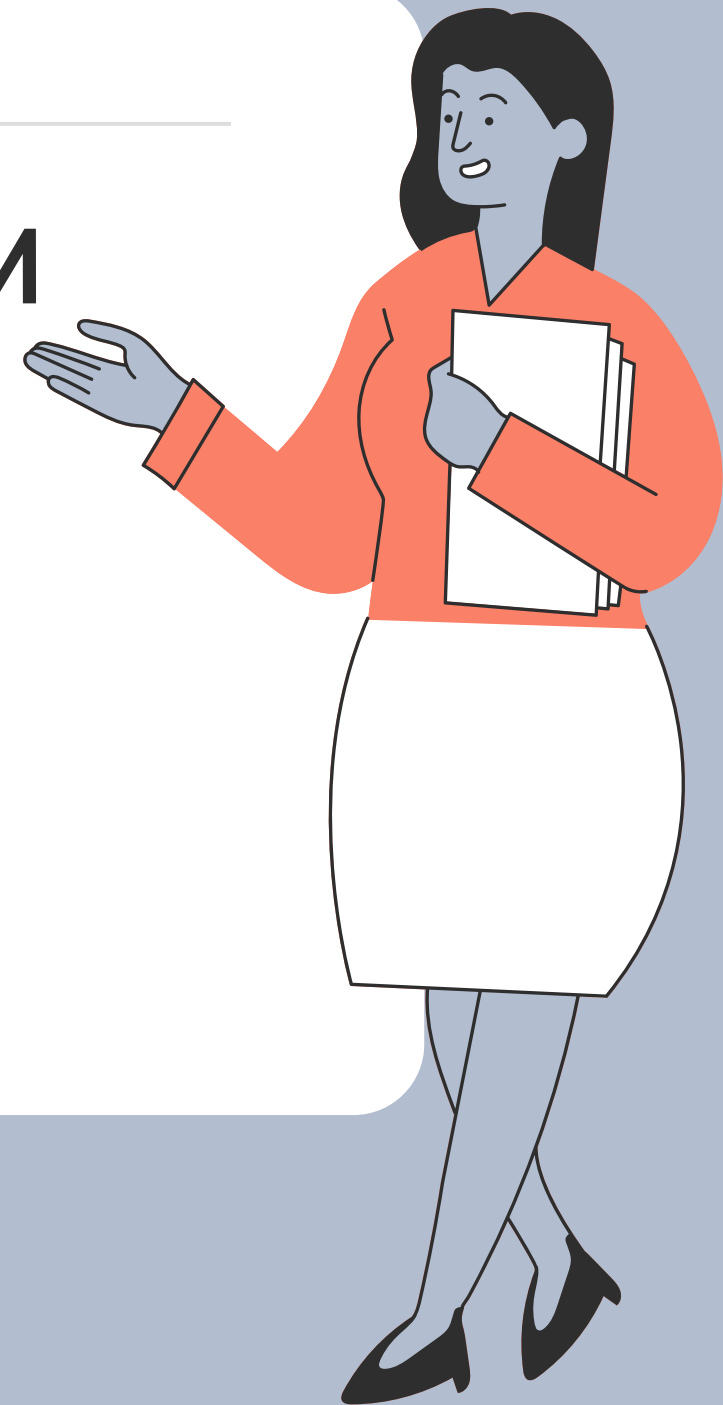
3. WHAT IS AUTO INGESTION OF DATA?

- Auto-ingest simply listens to the notifications from S3 and ingests new files as they arrive.

- It relies on SQS queues to deliver event notifications from S3 to Snowpipe.

AUTO INGESTION OF DATA IMPLEMENTATION

1. Created Snowpipe with auto-ingestion
2. Created Event Notification in AWS S3
3. Data will be loaded from stage to source table on receiving notification from S3
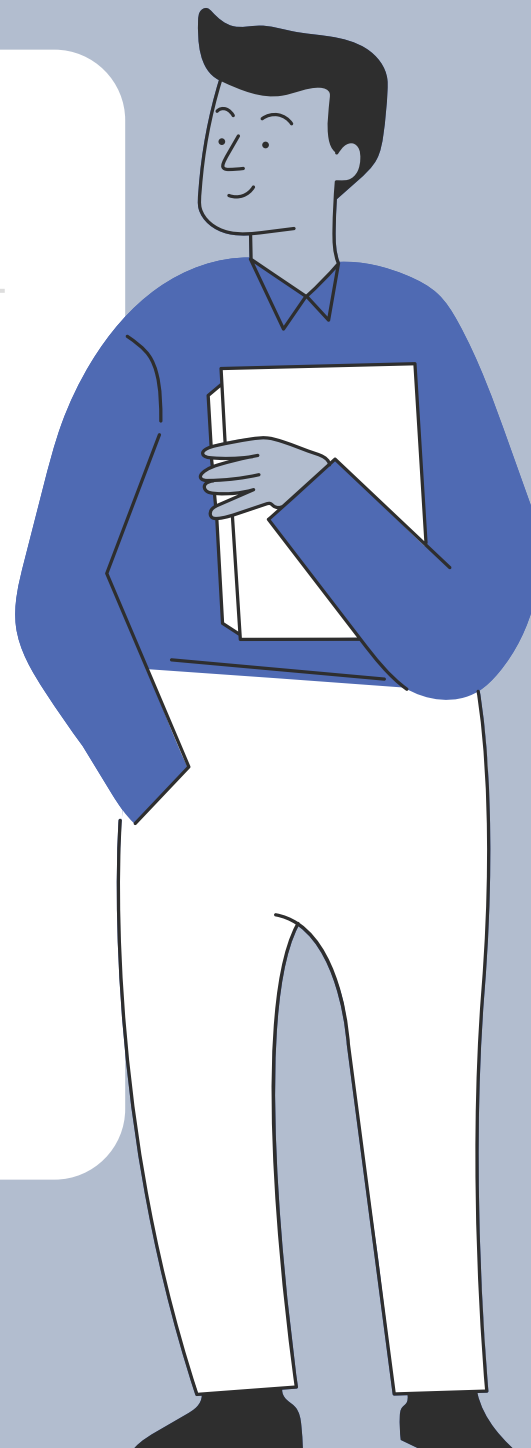
4. WHAT IS SLOWLY CHANGING DIMENSION?

- SCD is a dimension that change over the time
- SCD Type 2 :
    1. All Historical data is maintained
   2. New row is inserted every time an attribute changes
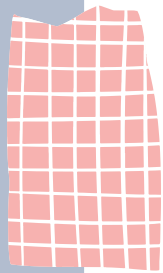
SLOWLY CHANGING DIMENSION IMPLEMENTATION

1. Created a stream to capture DML changes made to the source table
2. Created a task to merge data into target table
3. Displayed the target table that will return all the records with versioning history
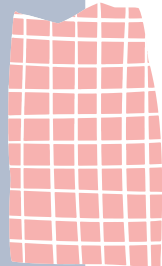
5. WHAT IS COLUMN LEVEL MASKING?

- Works on column within a table or view.

- It assigns the MASKED attribute to columns so that unprivileged users cannot view the data
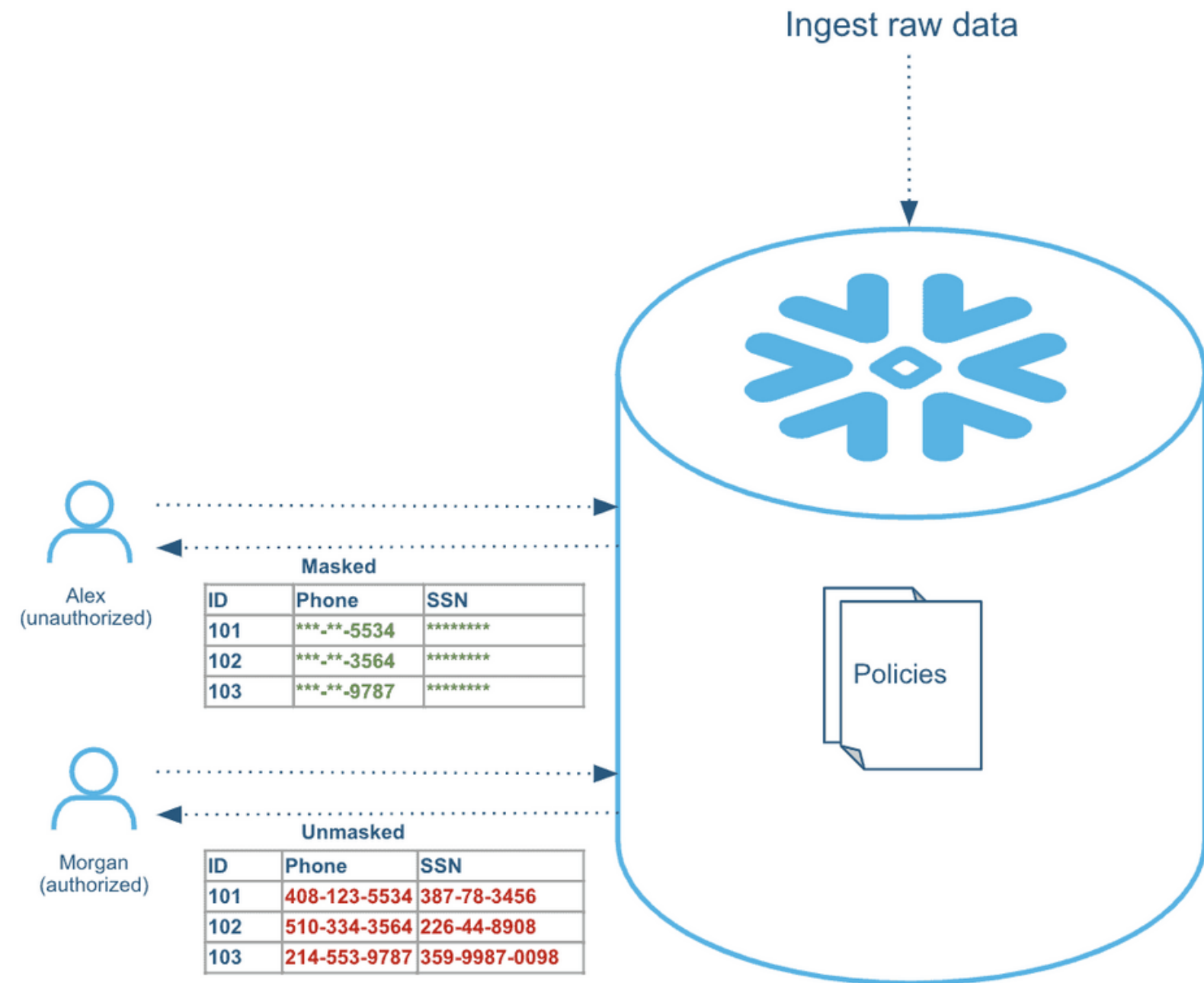
COLUMN LEVEL MASKING IMPLEMENTATION

1. Created a new role (superstore_role)
2. Created masking policy
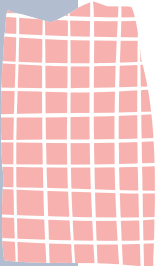3. Masked sensitive columns from target table when viewed from any other role.

6. WHAT IS ROW LEVEL SECURITY?

- **Access to data is limited according to certain restrictions.**

- **Various users or roles have different permissions on certain rows, based on identities within the rows.**
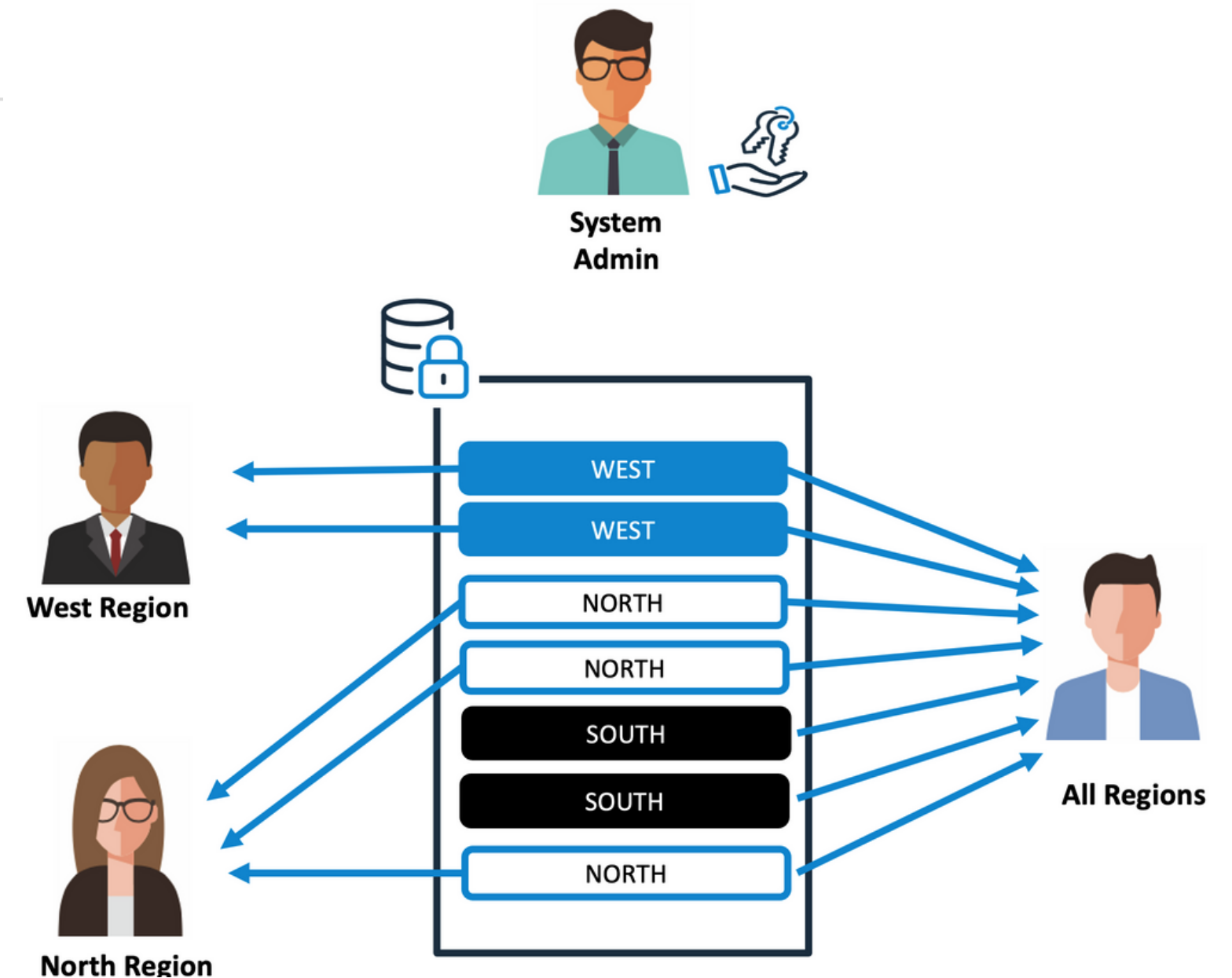
ROW LEVEL SECURITY IMPLEMENTATION

1. Created roles based on a relevant column
2. Created users with their default roles
3. Granted secure view of respective entries/rows to the roles.

THANK YOU!

Any Questions