**1.3 OLS, CLS, RLS, File-level access control**

A screen shot of a computer

AI-generated content may be incorrect.

Key points

* You can apply object-level security (OLS), or column-level security (CLS) OR row-level security (RLS) to tables via the Lakehouse T-SQL analytics endpoint and/ or the Data Warehouse (most common in the Data Warehouse).
* Or granular OLS/ CLS/ RLS can be defined in semantic models also, but this section of the exam is focused on implementing OLS/CLS/RLS in a Data Warehouse/ T-SQL Endpoint of a Lakehouse.
* Note: if you apply OLS/CLS/RLS in a Data Warehouse - these settings do not propagate into a semantic model that reads from this Data Warehouse. Meaning, you will have to set up OLS/CLS/RLS in the Semantic Model too - they are not linked, currently, I believe Q1, 2025, they plan to release Universal Security, which seeks to tackle this problem.
* Note 2: Power BI queries on a warehouse table (with an active RLS policy) in Direct Lake mode will fall back to Direct Query mode to abide by row-level security.
* File-level access control is given using OneLake Data Access model - in the Lakehouse (because Files can only exist in the Lakehouse!).

**Implement OLS in a (Data Warehouse/Data Lakehouse T-SQL Endpoint)**

*Note: as a prerequisite, the user or role you want to apply OLS to must have Read permission ONLY, on the Data Warehouse. This means:*

* *they should NOT be given any workspace-level role*
* *you should share the Warehouse (item-level), with NO ADDITIONAL PERMISSIONS, like in the screenshot below:*

A screenshot of a computer

AI-generated content may be incorrect.

For OLS, use a GRANT statement, like this, to give the user (or role) SELECT permissions on the table:

A screenshot of a computer

AI-generated content may be incorrect.GRANT SELECT ON Sales.Orders TO [SalesReps];

Note:

* GRANT: gives the user/role permission to access specific table or all tables in a schema.
* DENY: explicitly block access to specific table(s) or all tables in a schema.
* REVOKE: removes the previous GRANT/DENY rule you set on table(s) or all tables in a schema.

**Implement CLS in a (Data Warehouse/Data Lakehouse T-SQL Endpoint)**

*Note: as a prerequisite, the user or role you want to apply CLS to must have Read permission ONLY, on the Data Warehouse. This means:*

* *they should NOT be given any workspace-level role*
* *you should share the Warehouse (item-level), with NO ADDITIONAL PERMISSIONS, like in the screenshot below:*

A screenshot of a computer

AI-generated content may be incorrect.

For CLS, use a GRANT statement, like below, to give the user (or role) SELECT permissions on specific columns in a specific table:

GRANT SELECT (CustomerId, AccountCreationDate) ON Sales.CustomerDetails

TO [SalesReps];

A screenshot of a computer

AI-generated content may be incorrect.

**Apply RLS to a Warehouse table (three steps)**

*Prerequisite: the user (or role), must have the ability to read the table before you apply RLS, this can be given through ReadData permissions, or Read permissions plus Granting SELECT (OLS) on the table of interest.*

1. Create a schema for all your security-related things (called Security) - this is optional, but it's good to keep all security-related assets in one schema.

CREATE SCHEMA Security;

1. Create a T-SQL Function, which filters the rows in a given table, based on the logged-in user's USER\_NAME(), returning the filtered table.

*Note: it also returns the rows if you are a member of the 'manager' role, for convenience.*

CREATE FUNCTION Security.f\_FilterRowsForLoggedInUser(@SalesRep AS varchar(100))

RETURNS TABLE

WITH SCHEMABINDING

AS

RETURN SELECT 1 AS f\_FilterResult

WHERE @SalesRep = USER\_NAME() OR IS\_ROLEMEMBER('manager') = 1;

GO;

1. Set up a SECURITY POLICY to apply the function to the table

CREATE SECURITY POLICY SalesRowFilterPolicy

ADD FILTER PREDICATE Security.f\_FilterRowsForLoggedInUser(SalesRep)

ON Sales.Orders

WITH (STATE = ON);

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**Implement file-based access (to Lakehouse folders - PREVIEW)**

Workspace admins, members, and contributors are able to modify access to Lakehouse objects, at the folder level. To start, click on this button in the ribbon:

1. Create a role and specify which tables and files you want to give the role access to:

A screenshot of a computer

AI-generated content may be incorrect.

1. Add people or groups to the Role

A screenshot of a computer

AI-generated content may be incorrect.

A screen shot of a computer security

AI-generated content may be incorrect.**OneLake Security (PREVIEW)**

Note:

A screenshot of a computer

AI-generated content may be incorrect.