Question #101 *Topic 1*

A company needs to share its product catalog data with one of its partners. The product catalog data is stored in two database tables: PRODUCT_CATEGORY, and PRODUCT_DETAILS. Both tables can be joined by the PRODUCT_ID column. Data access should be governed, and only the partner should have access to the records.

The partner is not a Snowflake customer. The partner uses Amazon S3 for cloud storage.

Which design will be the MOST cost-effective and secure, while using the required Snowflake features?

A. Use Secure Data Sharing with an S3 bucket as a destination.

B. Publish PRODUCT_CATEGORY and PRODUCT_DETAILS data sets on the Snowflake Marketplace.

C. Create a database user for the partner and give them access to the required data sets.

D. Create a reader account for the partner and share the data sets as secure views.

Correct Answer: *D*

Community vote distribution

D (100%)

Question #102 *Topic 1*

A company has a Snowflake environment running in AWS us-west-2 (Oregon). The company needs to share data privately with a customer who is running their Snowflake environment in Azure East US 2 (Virginia).

What is the recommended sequence of operations that must be followed to meet this requirement?

A. 1. Create a share and add the database privileges to the share
2. Create a new listing on the Snowflake Marketplace
3. Alter the listing and add the share
4. Instruct the customer to subscribe to the listing on the Snowflake Marketplace

B. 1. Ask the customer to create a new Snowflake account in Azure EAST US 2 (Virginia)
2. Create a share and add the database privileges to the share
3. Alter the share and add the customer's Snowflake account to the share

C. 1. Create a new Snowflake account in Azure East US 2 (Virginia)
2. Set up replication between AWS us-west-2 (Oregon) and Azure East US 2 (Virginia) for the database objects to be shared
3. Create a share and add the database privileges to the share
4. Alter the share and add the customer's Snowflake account to the share

D. 1. Create a reader account in Azure East US 2 (Virginia)
2. Create a share and add the database privileges to the share
3. Add the reader account to the share
4. Share the reader account's URL and credentials with the customer

Correct Answer: *C*

Community vote distribution

C (100%)

Question #103 *Topic 1*

Company A has recently acquired company B. The Snowflake deployment for company B is located in the Azure West Europe region.

As part of the integration process, an Architect has been asked to consolidate company B's sales data into company A's Snowflake account which is located in the AWS us-east-1 region.

How can this requirement be met?

A. Replicate the sales data from company B's Snowflake account into company A's Snowflake account using cross-region data replication within Snowflake. Configure a direct share from company B's account to company A's account.

B. Export the sales data from company B's Snowflake account as CSV files, and transfer the files to company A's Snowflake account. Import the data using Snowflake's data loading capabilities.

C. Migrate company B's Snowflake deployment to the same region as company A's Snowflake deployment, ensuring data locality. Then perform a direct database-to-database merge of the sales data.

D. Build a custom data pipeline using Azure Data Factory or a similar tool to extract the sales data from company B's Snowflake account. Transform the data, then load it into company A's Snowflake account.

Correct Answer: *A*

Community vote distribution

A (100%)

Question #104 *Topic 1*

A Snowflake Architect created a new data share and would like to verify that only specific records in secure views are visible within the data share by the consumers.

What is the recommended way to validate data accessibility by the consumers?

A. Create reader accounts as shown below and impersonate the consumers by logging in with their credentials.

create managed account reader_acct1 admin_name = user1 , admin_password = 'Sdfed43da!44' , type = reader;

B. Create a row access policy as shown below and assign it to the data share.

create or replace row access policy rap_acct as (acct_id varchar) returns boolean -> case when 'acct1_role' = current_role() then true else false end;

C. Set the session parameter called SIMULATED_DATA_SHARING_CONSUMER as shown below in order to impersonate the consumer accounts.

alter session set simulated_data_sharing_consumer = 'Consumer Acct1'

D. Alter the share settings as shown below, in order to impersonate a specific consumer account.

alter share sales_share set accounts = 'Consumer1' share_restrictions = true

Correct Answer: *C*

Community vote distribution

C (100%)

Question #105 *Topic 1*

A company is using Snowflake in Azure in the Netherlands. The company analyst team also has data in JSON format that is stored in an Amazon S3 bucket in the AWS Singapore region that the team wants to analyze.

The Architect has been given the following requirements:

1. Provide access to frequently changing data
2. Keep egress costs to a minimum
3. Maintain low latency

How can these requirements be met with the LEAST amount of operational overhead?

A. Use a materialized view on top of an external table against the S3 bucket in AWS Singapore.

B. Use an external table against the S3 bucket in AWS Singapore and copy the data into transient tables.

C. Copy the data between providers from S3 to Azure Blob storage to collocate, then use Snowpipe for data ingestion.

D. Use AWS Transfer Family to replicate data between the S3 bucket in AWS Singapore and an Azure Netherlands Blob storage, then use an external table against the Blob storage.

Correct Answer: *C*

Community vote distribution

A (75%) D (25%)

Question #106 *Topic 1*

Based on the Snowflake object hierarchy, what securable objects belong directly to a Snowflake account? (Choose three.)

A. Database

B. Schema

C. Table

D. Stage

E. Role

F. Warehouse

Correct Answer: *AEF*

Community vote distribution

AEF (100%)

Question #107 *Topic 1*

What is a characteristic of Role-Based Access Control (RBAC) as used in Snowflake?

A. Privileges can be granted at the database level and can be inherited by all underlying objects.

B. A user can use a "super-user" access along with SECURITYADMIN to bypass authorization checks and access all databases, schemas, and underlying objects.

C. A user can create managed access schemas to support future grants and ensure only schema owners can grant privileges to other roles.

D. A user can create managed access schemas to support current and future grants and ensure only object owners can grant privileges to other roles.

Correct Answer: *C*

Community vote distribution

C (100%)

Question #108 *Topic 1*

Assuming all Snowflake accounts are using an Enterprise edition or higher, in which development and testing scenarios would copying of data be required, and zero-copy cloning not be suitable? (Choose two.)

A. Developers create their own datasets to work against transformed versions of the live data.

B. Production and development run in different databases in the same account, and Developers need to see production-like data but with specific columns masked. Most Voted

C. Data is in a production Snowflake account that needs to be provided to Developers in a separate development/testing Snowflake account in the same cloud region. Most Voted

D. Developers create their own copies of a standard test database previously created for them in the development account, for their initial development and unit testing.

E. The release process requires pre-production testing of changes with data of production scale and complexity. For security reasons, pre-production also runs in the production account.

Correct Answer: *BC*

Community vote distribution

BC (100%)

A new user user_01 is created within Snowflake. The following two commands are executed:

Command 1 –> show grants to user user_01;
Command 2 –> show grants on user user_01;

What inferences can be made about these commands?

A. Command 1 defines which user owns user_01
Command 2 defines all the grants which have been given to user_01

B. Command 1 defines all the grants which are given to user_01
Command 2 defines which user owns user_01

C. Command 1 defines which role owns user_0l
Command 2 defines all the grants which have been given to user_01 Most Voted

D. Command 1 defines all the grants which are given to user_01
Command 2 defines which role owns user_01

Correct Answer: *C*

Community vote distribution

C (75%) D (25%)

Previous Questions