Free Questions for ADA-C01

Shared by Kirkland on 16-04-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What roles can be used to create network policies within Snowflake accounts? (Choose THREE).

Options:

A- SYSADMIN
B- SECURITYADMIN
C- ACCOUNTADMIN
D- ORGADMIN
E- Any role with the global permission of CREATE NETWORK POLICY
F- Any role that owns the database where the network policy is created

Answer:

B, C, E

Explanation:

Network policies are used to restrict access to the Snowflake service and internal stages based on user IP address1. To create network policies, a role must have the global permission of CREATE NETWORK POLICY2. By default, the system-defined roles of SECURITYADMIN and ACCOUNTADMIN have this permission3. However, any other role can be granted this permission by an administrator4. Therefore, the answer is B, C, and E. The other options are incorrect because SYSADMIN and ORGADMIN do not have the CREATE NETWORK POLICY permission by default3, and network policies are not tied to specific databases5.

Question 2

Question Type: MultipleChoice

If the query matches the definition, will Snowflake always dynamically rewrite the query to use a materialized view?

Options:

A- No, because joins are not supported by materialized views.

B- No, because the optimizer might decide against it.
C- No, because the materialized view may not be up-to-date.
D- Yes, because materialized views are always faster.

Answer:

B

Explanation:

Snowflake's query optimizer can automatically rewrite queries against the base table or regular views to use the materialized view instead, if the query matches the definition of the materialized view1. However, this is not always guaranteed, as the optimizer might decide against using the materialized view based on various factors, such as the freshness of the data, the size of the result set, the complexity of the query, and the availability of the materialized view2. Therefore, the answer is no, because the optimizer might decide against it.

Question 3

Question Type: MultipleChoice

An Administrator receives data from a Snowflake partner. The partner is sharing a dataset that contains multiple secure views. The Administrator would like to configure the

data so that only certain roles can see certain secure views.

How can this be accomplished?

Options:

A- Apply RBAC directly onto the partner's shared secure views.
B- Individually grant imported privileges onto the schema in the share.
C- Clone the data and insert it into a company-owned share and apply the desired RBAC on the new tables.
D- Create views over the incoming shared database and apply the desired RBAC onto these views.

Answer:

D

Explanation:

According to the Snowflake documentation1, secure views are only exposed to authorized users who have been granted the role that owns the view. Therefore, applying RBAC directly onto the partner's shared secure views (option A) is not possible, as the administrator does not own those views. Individually granting imported privileges onto the schema in the share (option B) is also not feasible, as the privileges granted on the schema do not apply to existing secure views, only to future ones2. Cloning the data and inserting it into a company-owned share (option C) is not recommended, as it would create unnecessary duplication of data and increase storage costs. The best option is to create views over the incoming shared database and apply the desired RBAC onto these views (option D). This way, the administrator can control the access to the data based on the roles in their account, without modifying the original data or views from the partner.

Question 4

Question Type: MultipleChoice

A virtual warehouse report_wh is configured with AUTO_RESUME=TRUE and AUTO_SUSPEND=300. A user has been granted the role accountant.

An application with the accountant role should use this warehouse to run financial reports, and should keep track of compute credits used by the warehouse.

What minimal privileges on the warehouse should be granted to the role to meet the requirements for the application? (Select TWO).

Options:

A- OPERATE
B- MODIFY
C- MONITOR
D- USAGE
E- OWNERSHIP

Answer:

C, D

Explanation:

According to the Snowflake documentation1, the MONITOR privilege on a warehouse grants the

ability to view the warehouse usage and performance metrics, such as the number of credits consumed, the average and maximum run time, and the number of queries executed. The USAGE privilege on a warehouse grants the ability to use the warehouse to execute queries and load data. Therefore, the minimal privileges on the warehouse that should be granted to the role to meet the requirements for the application are MONITOR and USAGE. Option A is incorrect because the OPERATE privilege on a warehouse grants the ability to start, stop, resume, and suspend the warehouse, which is not required for the application. Option B is incorrect because the MODIFY privilege on a warehouse grants the ability to alter the warehouse properties, such as the size, auto-suspend, and auto-resume settings, which is not required for the application. Option E is incorrect because the OWNERSHIP privilege on a warehouse grants the ability to drop the warehouse, grant or revoke privileges on the warehouse, and transfer the ownership to another role, which is not required for the application.

P2P exams