

Snowflake NAS-C01 Dumps PDF And Practice Test Software



Our Snowflake NAS-C01 test braindump materials is popular based on that too. As we all know the passing rate for exams is low, the wise choice for candidates will select valid Snowflake NAS-C01 test braindump materials to make you pass exam surely and fast. Our Snowflake NAS-C01 test simulations will help you twice the result with half the effort.

We know that once we sell fake products to customers, we will be knocked out by the market. So we strongly hold the belief that the quality of the NAS-C01 practice materials is our lifeline. When you begin practicing our NAS-C01 study materials, you will find that every detail of our NAS-C01 study questions is wonderful. Because that we have considered every detail on the developing the exam braindumps, not only on the designs of the content but also on the displays.

>> NAS-C01 Test Result <<

Reliable NAS-C01 Practice Materials, Free NAS-C01 Braindumps

DumpsTests guarantees its customers that they will pass the NAS-C01 exam on their first attempt. DumpsTests guarantees that you will receive a refund if you fail the Snowflake NAS-C01 Exam. For assistance with Snowflake NAS-C01 exam preparation and practice, DumpsTests offers its users three formats.

Snowflake SnowPro Specialty - Native Apps Sample Questions (Q77-Q82):

NEW QUESTION # 77

A data science company is developing a Snowflake Native App that provides advanced fraud detection for financial institutions. The app requires secure access to sensitive transaction data within the consumer's Snowflake account. Which of the following approaches BEST aligns with Snowflake's recommended practices for managing data access and securing data within a Native App?

- A. The app should request full ACCOUNTADMIN privileges in the consumer account to access all necessary data for fraud detection.
- B. The app should use secure views created by the consumer that grant the app read-only access to only the specific transaction data needed for fraud detection.

- C. The app should directly access tables containing transaction data using the consumer's own service account credentials, which are securely stored within the app's code.
- D. The app should create and manage its own temporary tables in the consumer account and load transaction data into them for processing.
- E. The app should directly access transaction data through data sharing from provider account.

Answer: B

Explanation:

Using secure views is the best approach. Secure views allow the consumer to control precisely what data the application can access without granting overly broad permissions. This minimizes the risk of unintended data exposure and adheres to the principle of least privilege. ACCOUNTADMIN is excessive and insecure. Storing credentials is also insecure and against best practices. Creating temporary tables and loading data duplicates data and can be inefficient.

NEW QUESTION # 78

You're developing a Snowflake Native App that interacts with a REST API. The API key needs to be securely stored and accessed within your application. Which of the following approaches provide the MOST secure and manageable way to handle the API key?

- A. Store the API key in a separate configuration file uploaded to a stage, encrypting the file with a symmetric key hardcoded in the application.
- B. Store the API key directly in the application code as a constant variable.
- C. Store the API key in a secure vault (e.g., HashiCorp Vault) and use an external function to retrieve the key at runtime. Implement appropriate authentication and authorization for the external function.
- D. Store the API key as an environment variable in the Snowflake environment.
- E. Use Snowflake Secrets to store the API key securely and grant access to the APPLICATION role. Then, access the secret within your Stored Procedure or UDF.

Answer: E

Explanation:

Snowflake Secrets are designed for securely storing sensitive information like API keys. Granting access to the APPLICATION role ensures that only the application code can access the key. Storing keys directly in code or configuration files, even encrypted ones, is a security risk. Environment variables in Snowflake are not a secure storage mechanism for sensitive data. An external vault adds significant complexity to a Snowflake Native App.

NEW QUESTION # 79

You are developing a Snowflake Native Application that requires secure access to external services for data enrichment. You choose to implement an External Function with API Integration. Which of the following security best practices are MOST important to implement when configuring the API Integration and the External Function to minimize security risks?

- A. Store any sensitive credentials required by the external service directly in the External Function's code body for easy access.
- B. Grant usage on the API integration to PUBLIC role to allow all users to invoke the external function.
- C. Disable network policies on the API Integration to avoid accidental blocking of traffic.
- D. Configure 'AWS IAM ROLE ARNS or similar parameters (depending on cloud provider) to grant Snowflake the least privilege access to the specific resources on the external service required by the function.
- E. Use the parameter in the API Integration to restrict access to only the trusted IP addresses of the external service.

Answer: D,E

Explanation:

Options B and D are correct. Using restricts the allowed source IPs for connection to the External Function, reducing the attack surface. Using 'AWS IAM ROLE ARN' (or equivalent) with the principle of least privilege ensures that Snowflake only has the necessary permissions on the external service, minimizing the potential impact of a compromised function. Option A is incorrect because granting usage to PUBLIC is a security risk. Option C is incorrect because storing credentials directly in code is a bad practice. Option E is incorrect because network policies should be in place for security. The other options either create a broad attack surface or directly expose sensitive information.

NEW QUESTION # 80

A data science team is developing a Native App on Snowflake that requires access to data from multiple customer accounts (Reader Accounts). They need to ensure strict data governance and minimize the risk of data leakage. Which of the following approaches provides the MOST secure and scalable solution for accessing and managing this cross-account data?

- A. Grant SELECT privileges directly to the application role on all relevant tables in the consumer accounts.
- B. Implement a data access service within the Native App that uses external functions to query data from consumer accounts, relying on network policies for security.
- C. Package the data extraction logic directly into the Native App using User-Defined Functions (UDFs) that establish secure connections to each consumer account using separate credentials stored securely within the application package.
- D. Create a shared database from each consumer account containing views over the required tables, granting SELECT privileges on these views to the application role.
- E. Utilize secure data sharing with data clean rooms, exposing the required datasets via views on each data clean room.

Answer: E

Explanation:

Secure data sharing provides the MOST secure and scalable solution. Data clean rooms add governance, limiting what data can be exposed, and simplifying setup. Options A and B expose data without fine-grained control; Option C introduces complexities with external function setup and network policies; Option D raises security concerns by managing consumer credentials within the application.

NEW QUESTION # 81

You are packaging a Snowflake Native App and need to ensure that consumer accounts can only access specific data views you've created within your application schema. You want to prevent consumers from directly querying the underlying tables. Which of the following security measures, when implemented together, BEST achieve this objective? (Choose two)

- A. Do not grant any privileges on the underlying tables to the 'application role' within the application package.
- B. Grant 'SELECT' privilege on the underlying tables to the 'application role' within the application package.
- C. Grant 'SELECT privilege only on the views to the 'application role' within the application package.
- D. Grant 'OWNERSHIP' on the views to the 'application role' within the application package.
- E. Use secure views to expose data, ensuring data access is controlled through the view's definition.

Answer: C,E

Explanation:

The combination of granting 'SELECT' only on the views (Option B) and using secure views (Option E) provides the strongest data security. Granting select on the views allows consumers to see the data you want them to see. Secure views prevent consumers from circumventing the view definition to access underlying tables, even if they had theoretical privileges (which they shouldn't). Not granting any privileges on tables (C) is correct in conjunction with (B&E), but on its own consumers will not see any data as they can't select from any object. Giving application role ownership to View (D) is not necessary to give consumer access to view the data.

NEW QUESTION # 82

.....

Now in such a Internet so developed society, choosing online training is a very common phenomenon. DumpsTests is one of many online training websites. DumpsTests's online training course has many years of experience, which can provide high quality learning material for examinee participating in Snowflake Certification NAS-C01 Exam and satisfy all the needs of the students.

Reliable NAS-C01 Practice Materials: <https://www.dumpstests.com/NAS-C01-latest-test-dumps.html>

Snowflake NAS-C01 Test Result We are all well aware that a major problem in the industry is that there is a lack of quality study materials, For exam candidates it is of great importance to pass the Snowflake Reliable NAS-C01 Practice Materials exams effectively, Snowflake NAS-C01 Test Result Discounts unregularly, Snowflake NAS-C01 Test Result Since everyone knows certificate exams are difficult to pass.

The list of valid key words depends on the policy enforced, What led you to becoming NAS-C01 a prolific writer of technical books, We are all well aware that a major problem in the industry is that there is a lack of quality study materials.

