ARA-C01試験問題 & ARA-C01日本語版試験解答

さらに、Japancert ARA-C01ダンプの一部が現在無料で提供されています：https://drive.google.com/open?id=1YJGAv1Dns4_5R-rM0J_we419kwAfB4_k

長い間ARA-C01認定を希望しているかもしれませんが、Snowflake勉強する時間や良い方法がありません。勉強はつまらないと思っていたのかもしれません。 ARA-C01の学習教材があなたの心を変えます。当社の製品を使用すると、すぐに勉強の幸せを感じるでしょう。熱心なJapancert専門家のおかげで、ARA-C01試験に合格するためのすばらしい学習ツールが考案されました。最初にデモを試してみると、勉強をやめられないことがわかります。 ARA-C01学習教材を使用すると、自分自身に挑戦して、もっと知りたいと思うでしょう。

Snowflake ARA-C01認定を獲得するには、候補者は、スノーフレークアーキテクチャと機能に関連する幅広いトピックをカバーする厳格な試験に合格する必要があります。この試験は、60の複数選択の質問で構成され、90分間タイミングが合っています。この試験はコンピューターベースであり、候補者の自宅またはオフィスから認可されたテストセンターまたはリモートで撮影できます。

>> ARA-C01試験問題 <<

ARA-C01日本語版試験解答、ARA-C01トレーニング資料

Japancert製品を購入する前にARA-C01学習ツールの無料ダウンロードと試用を提供し、製品のデモを提供して、クライアントに製品を完全に知らせます。 WebサイトのARA-C01テストトレントのページにアクセスすると、ARA-C01ガイドトレントの特性とメリットを知ることができます。 Webサイトの製品のページでは、詳細と保証、連絡方法、ARA-C01テストトレントでのクライアントの評価、およびARA-C01試験問題に関するその他の情報を見つけることができます。とても便利です。

Snowflake ARA-C01 認定試験の出題範囲：

トピック	出題範囲
トピック 1	• 開発ライフサイクルとワークロード要件をサポートするアーキテクチャ ソリューションを作成する • Snowflake セキュリティ原則の概要を説明し、それらを適用する必要があるユースケースを特定する
トピック 2	• ビジネス要件に基づいて Snowflake アカウントとデータベース戦略を設計する • 既存のアーキテクチャのパフォーマンス問題のトラブルシューティング
トピック 3	• Snowflake 環境におけるさまざまなデータ モデルの利点と制限の概要を説明します。Snowflake のエコシステム内の主要なツールと、それらが Snowflake とどのように相互作用するかを説明します。

Snowflake SnowPro Advanced Architect Certification 認定 ARA-C01 試験問題 (Q101-Q106):

質問 # 101
A company has an inbound share set up with eight tables and five secure views. The company plans to make the share part of its production data pipelines.
Which actions can the company take with the inbound share? (Choose two.)

- A. Create additional views inside the shared database.
- B. Create a table from the shared database.
- C. Clone a table from a share.
- D. Grant modify permissions on the share.
- E. Create a table stream on the shared table.

正解：A、C

解説：
These two actions are possible with an inbound share, according to the Snowflake documentation and the web search results. An inbound share is a share that is created by another Snowflake account (the provider) and imported into your account (the consumer). An inbound share allows you to access the data shared by the provider, but not to modify or delete it. However, you can perform some actions with the inbound share, such as:
* Clone a table from a share. You can create a copy of a table from an inbound share using the CREATE TABLE ... CLONE statement. The clone will contain the same data and metadata as the original table,
* but it will be independent of the share. You can modify or delete the clone as you wish, but it will not reflect any changes made to the original table by the provider1.
* Create additional views inside the shared database. You can create views on the tables or views from an inbound share using the CREATE VIEW statement. The views will be stored in the shared database, but they will be owned by your account. You can query the views as you would query any other view in your account, but you cannot modify or delete the underlying objects from the share2.
The other actions listed are not possible with an inbound share, because they would require modifying the share or the shared objects, which are read-only for the consumer. You cannot grant modify permissions on the share, create a table from the shared database, or create a table stream on the shared table34.
References:
* Cloning Objects from a Share | Snowflake Documentation
* Creating Views on Shared Data | Snowflake Documentation
* Importing Data from a Share | Snowflake Documentation
* Streams on Shared Tables | Snowflake Documentation

質問 # 102
Which Snowflake data modeling approach is designed for BI queries?

- A. Data Vault
- B. 3 NF
- C. Snowflake schema
- D. Star schema

正解：C

質問 # 103
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. Copy the data between providers from S3 to Azure Blob storage to collocate, then use Snowpipe for data ingestion.
- C. Use an external table against the S3 bucket in AWS Singapore and copy the data into transient tables.
- 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.

正解：C

質問 # 104
A company has an external vendor who puts data into Google Cloud Storage. The company's Snowflake account is set up in Azure. What would be the MOST efficient way to load data from the vendor into Snowflake?

- A. Ask the vendor to create a Snowflake account, load the data into Snowflake and create a data share.
- B. Copy the data from Google Cloud Storage to Azure Blob storage using external tools and load data from Blob storage to Snowflake.
- C. Create an external stage on Google Cloud Storage and use the external table to load the data into Snowflake.
- D. Create a Snowflake Account in the Google Cloud Platform (GCP), ingest data into this account and use data replication to move the data from GCP to Azure.

正解：C

解説：
The most efficient way to load data from the vendor into Snowflake is to create an external stage on Google Cloud Storage and use the external table to load the data into Snowflake (Option B). This way, you can avoid copying or moving the data across different cloud platforms, which can incur additional costs and latency. You can also leverage the external table feature to query the data directly from Google Cloud Storage without loading it into Snowflake tables, which can save storage space and improve performance. Option A is not efficient because it requires the vendor to create a Snowflake account and a data share, which can be complicated and costly. Option C is not efficient because it involves copying the data from Google Cloud Storage to Azure Blob storage using external tools, which can be slow and expensive. Option D is not efficient because it requires creating a Snowflake account in the Google Cloud Platform (GCP), ingesting data into this account, and using data replication to move the data from GCP to Azure, which can be complex and time-consuming. Reference: The answer can be verified from Snowflake's official documentation on external stages and external tables available on their website. Here are some relevant links:
Using External Stages | Snowflake Documentation
Using External Tables | Snowflake Documentation
Loading Data from a Stage | Snowflake Documentation

質問 # 105
What is a characteristic of Role-Based Access Control (RBAC) as used in Snowflake?

- A. A user can create managed access schemas to support future grants and ensure only schema owners can grant privileges to other roles.
- B. Privileges can be granted at the database level and can be inherited by all underlying objects.
- C. A user can use a "super-user" access along with securityadmin to bypass authorization checks and access all databases, schemas, and underlying objects.
- 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.

正解：A、B

解説：
Role-Based Access Control (RBAC) is the Snowflake Access Control Framework that allows privileges to be granted by object owners to roles, and roles, in turn, can be assigned to users to restrict or allow actions to be performed on objects. A characteristic of RBAC as used in Snowflake is:
Privileges can be granted at the database level and can be inherited by all underlying objects. This means that a role that has a certain privilege on a database, such as CREATE SCHEMA or USAGE, can also perform the same action on any schema, table, view, or other object within that database, unless explicitly revoked. This simplifies the access control management and reduces the number of grants required.
A user can create managed access schemas to support future grants and ensure only schema owners can grant privileges to other roles. This means that a user can create a schema with the MANAGED ACCESS option, which changes the default behavior of

object ownership and privilege granting within the schema. In a managed access schema, object owners lose the ability to grant privileges on their objects to other roles, and only the schema owner or a role with the MANAGE GRANTS privilege can do so. This enhances the security and governance of the schema and its objects.
The other options are not characteristics of RBAC as used in Snowflake:
A user can use a "super-user" access along with securityadmin to bypass authorization checks and access all databases, schemas, and underlying objects. This is not true, as there is no such thing as a "super-user" access in Snowflake. The securityadmin role is a predefined role that can manage users and roles, but it does not have any privileges on any database objects by default. To access any object, the securityadmin role must be explicitly granted the appropriate privilege by the object owner or another role with the grant option.
A user can create managed access schemas to support current and future grants and ensure only object owners can grant privileges to other roles. This is not true, as this contradicts the definition of a managed access schema. In a managed access schema, object owners cannot grant privileges on their objects to other roles, and only the schema owner or a role with the MANAGE GRANTS privilege can do so.
Reference:
Overview of Access Control
A Functional Approach For Snowflake's Role-Based Access Controls
Snowflake Role-Based Access Control simplified
Snowflake RBAC security prefers role inheritance to role composition
Overview of Snowflake Role Based Access Control

質問 # 106
......

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, Disposable vapes

P.S.JapancertがGoogle Driveで共有している無料の2026 Snowflake ARA-C01ダンプ：https://drive.google.com/open?id=1YJGAv1Dns4_5R-rM0J_we419kwAfB4_k