ADA-C01 Free Pdf Guide, ADA-C01 Valid Test Discount

2026 Latest Itcertking ADA-C01 PDF Dumps and ADA-C01 Exam Engine Free Share: https://drive.google.com/open?id=1L_qz8R0ogO0KgDiX2wRSAW6J6PrtqLCP

If you do all things with efficient, you will have a promotion easily. If you want to spend less time on preparing for your ADA-C01 exam, if you want to pass your exam and get the certification in a short time, our ADA-C01 Study Materials will be your best choice to help you achieve your dream. Only studying with our ADA-C01 learning engine for 20 to 30 hours, we can claim that you can pass you exam without difficulty.

Snowflake ADA-C01 Exam Syllabus Topics:

Topic	Details
Topic 1	• Performance Monitoring and Tuning: This section of the exam measures the skills of Cloud Infrastructure Engineers and Performance Analysts and focuses on optimizing Snowflake compute and storage resources. Candidates will need to understand how to configure and manage virtual warehouses, evaluate query profiles, and apply caching and clustering strategies for performance tuning. It also includes monitoring concurrency, resource utilization, and implementing cost optimization strategies. The ability to interpret, explain plans, apply search optimization, and manage cost controls is key for maintaining efficient Snowflake environments.
Topic 2	• Data Sharing, Data Exchange, and Snowflake Marketplace: This section of the exam measures the skills of Data Integration Specialists and Data Platform Administrators and covers managing and implementing data-sharing solutions within Snowflake. It evaluates understanding of data sharing models across regions and clouds, secure data sharing methods, and managing provider-consumer relationships. The domain also includes the use of Snowflake Data Exchange and Marketplace to publish, consume, and manage data listings, ensuring secure collaboration and efficient data monetization.

Topic 3	• Snowflake Security, Role-Based Access Control (RBAC), and User Administration: This section of the exam measures the skills of Snowflake Administrators and Cloud Security Engineers and covers authentication, access control, and network management in Snowflake. Candidates must understand how to configure authentication methods such as SSO, MFA, OAuth, and key-pair authentication, and how to manage network policies and private connectivity. The domain also tests knowledge of user and role management using SCIM, designing access control architecture, and applying the RBAC framework to ensure secure user authorization and data protection within Snowflake environments.
Topic 4	• Account Management and Data Governance: This section of the exam measures the skills of Data Governance Managers and Database Administrators and covers account organization, access control, and regulatory data protection. Candidates will learn how to manage organizational accounts, encryption keys, and Tri-Secret Secure implementations. It focuses on applying best practices in ORGADMIN and ACCOUNTADMIN roles, implementing masking and row access policies, and performing data classification and tagging. The domain also emphasizes data auditing, account identifiers, and effective management of tables, views, and query operations to support enterprise-wide governance standards.
Topic 5	• Disaster Recovery, Backup, and Data Replication: This section of the exam measures the skills of Disaster Recovery Engineers and Cloud Operations Managers and covers Snowflake methods for ensuring business continuity. Candidates must understand how to replicate databases and account-level objects, implement failover strategies, and perform backup and restoration through Time Travel and Fail-safe features. The domain emphasizes replication across accounts, handling data consistency during failover, and applying cost-efficient disaster recovery strategies to maintain availability during outages or regional failures.

ADA-C01 Valid Test Discount & Pdf ADA-C01 Exam Dump

With the help of performance reports of SnowPro Advanced Administrator (ADA-C01) Desktop practice exam software, you can gauge and improve your growth. You can also alter the duration and SnowPro Advanced Administrator (ADA-C01) questions numbers in your practice tests. Questions of this SnowPro Advanced Administrator (ADA-C01) mock test closely resemble the format of the actual test. As a result, it gives you a feeling of taking the actual test.

Snowflake SnowPro Advanced Administrator Sample Questions (Q43-Q48):

NEW QUESTION # 43
Which commands can be performed by a user with the ORGADMIN role but not the ACCOUNTADMIN role? (Select TWO).

- A. SHOW REGIONS;
- B. SHOW USERS;
- C. GRANT ROLE ORGADMIN TO USER <username>;
- D. SHOW ORGANIZATION ACCOUNTS;
- E. SELECT SYSTEM$GLOBAL_ACCOUNT_SET_PARAMETER (
  'ACCOUNT LOCATOR',
  'ENABLE ACCOUNT DATABASE_REPLICATION',
  'true'
  );

Answer: D,E

Explanation:
Explanation
According to the Snowflake documentation1, the ORGADMIN role is a special system role that is responsible for managing operations at the organization level, such as creating and viewing accounts, enabling database replication, and setting global account parameters. The ACCOUNTADMIN role is a system role that is responsible for managing operations at the account level, such as creating and managing users, roles, warehouses, databases, and shares. Therefore, the commands that can be performed by the ORGADMIN role but not the ACCOUNTADMIN role are:
*SHOW ORGANIZATION ACCOUNTS: This command lists all the accounts in the organization and their properties, such as

region, edition, and status2. The ACCOUNTADMIN role can only show the current account and its properties using the SHOW ACCOUNTS command3.
*SELECT SYSTEM$GLOBAL_ACCOUNT_SET_PARAMETER: This function sets a global account parameter for an account in the organization, such as enabling account database replication4. The ACCOUNTADMIN role can only set local account parameters using the ALTER ACCOUNT command.
Option A is incorrect because the SHOW REGIONS command can be executed by any role, not just the ORGADMIN role.
Option B is incorrect because the SHOW USERS command can be executed by the ACCOUNTADMIN role, as well as any role that has been granted the MONITOR privilege on the account.
Option D is incorrect because the GRANT ROLE ORGADMIN TO USER <username> command can be executed by the ACCOUNTADMIN role, as well as any role that has been granted the ORGADMIN role1.

NEW QUESTION # 44
A Snowflake Administrator created a role ROLE_MANAGED_ACCESS and a schema SCHEMA_MANAGED_ACCESS as follows:
USE ROLE SECURITYADMIN;
CREATE ROLE ROLE_MANAGED_ACCESS;
GRANT ROLE ROLE_MANAGED_ACCESS TO ROLE SYSADMIN;
GRANT USAGE ON WAREHOUSE COMPUTE_WH TO ROLE ROLE_MANAGED_ACCESS;
GRANT ALL privileges ON DATABASE WORK TO ROLE ROLE_MANAGED_ACCESS;
USE ROLE ROLE_MANAGED_ACCESS;
CREATE SCHEMA SCHEMA_MANAGED_ACCESS WITH MANAGED ACCESS;
USE ROLE SECURITYADMIN;
GRANT SELECT, INSERT ON FUTURE TABLES IN SCHEMA SCHEMA MANAGED ACCESS to ROLE_MANAGED_ACCESS; The Administrator now wants to disable the managed access on the schema.
How can this be accomplished?

- A. ALTER SCHEMA SCHEMA MANAGED ACCESS DISABLE MANAGED ACCESS;
- B. USE ROLE ROLE_MANAGED_ACCESS;
  DROP SCHEMA WORK. SCHEMA MANAGED_ACCESS;
  CREATE SCHEMA SCHEMA_MANAGED_ACCESS WITHOUT MANAGED ACCESS;
  Then recreate all needed objects.
- C. REVOKE SELECT, INSERT ON FUTURE TABLES IN SCHEMA SCHEMA_MANAGED_ACCESS FROM ROLE_MANAGED_ACCESS; ALTER SCHEMA SCHEMA MANAGED ACCESS DISABLE MANAGED ACCESS;
- D. USE ROLE ROLE MANAGED_ACCESS;
  DROP SCHEMA WORK. SCHEMA_MANAGED_ACCESS;
  CREATE SCHEMA SCHEMA_MANAGED_ACCESS;
  Then recreate all needed objects.

Answer: A

Explanation:
Explanation
According to the Snowflake documentation1, you can change a managed access schema to a regular schema using the ALTER SCHEMA statement with the DISABLE MANAGED ACCESS keywords. This will disable the managed access feature on the schema and revert the access control to the default behavior. Option B is incorrect because dropping and recreating the schema will also delete all the objects and metadata in the schema, which is not necessary to disable the managed access. Option C is incorrect because revoking the privileges on the future tables from the role is not required to disable the managed access. Option D is incorrect because there is no WITHOUT MANAGED ACCESS option in the CREATE SCHEMA statement.

NEW QUESTION # 45
For Snowflake network policies, what will occur when the account_level and user_level network policies are both defined?

- A. The account_level policy will override the user_level policy.
- B. The user_level network policies will not be supported.
- C. The user_level policy will override the account_level policy.
- D. A network policy error will be generated with no definitions provided.

Answer: C

Explanation:
Explanation
According to the Network Policies documentation, a network policy can be applied to an account, a security integration, or a user. If there are network policies applied to more than one of these, the most specific network policy overrides more general network policies. The following summarizes the order of precedence:
*Account: Network policies applied to an account are the most general network policies. They are overridden by network policies applied to a security integration or user.
*Security Integration: Network policies applied to a security integration override network policies applied to the account, but are overridden by a network policy applied to a user.
*User: Network policies applied to a user are the most specific network policies. They override both accounts and security integrations.
Therefore, if both the account_level and user_level network policies are defined, the user_level policy will take effect and the account_level policy will be ignored. The other options are incorrect because:
*The account_level policy will not override the user_level policy, as explained above.
*The user_level network policies will be supported, as they are part of the network policyfeature.
*A network policy error will not be generated, as there is no conflict between the account_level and user_level network policies.

NEW QUESTION # 46
The ACCOUNTADMIN of Account 123 works with Snowflake Support to set up a Data Exchange. After the exchange is populated with listings from other Snowflake accounts, what roles in Account 123 are allowed to request and get data?

- A. Any role with IMPORT SHARE and CREATE DATABASE privileges
- B. Any role that the listing provider has designated as authorized
- C. Any role with USAGE privilege on the Data Exchange
- D. Only the ACCOUNTADMIN role, and no other roles

Answer: C

Explanation:
Explanation
To request and get data from a Data Exchange, the role in Account 123 must have the USAGE privilege on the Data Exchange object. This privilege allows the role to view the listings and request access to the data.
According to the Snowflake documentation, "To view the listings in a data exchange, a role must have the USAGE privilege on the data exchange object. To request access to a listing, a role must have the USAGE privilege on the data exchange object and the IMPORT SHARE privilege on the account." The other options are either incorrect or not sufficient to request and get data from a Data Exchange. Option A is incorrect, as the ACCOUNTADMIN role is not the only role that can request and get data, as long as other roles have the necessary privileges. Option C is incorrect, as the IMPORT SHARE and CREATE DATABASE privileges are not required to request and get data, but only to create a database from a share after the access is granted.
Option D is incorrect, as the listing provider does not designate the authorized roles in Account 123, but only approves or denies the requests from Account 123.

NEW QUESTION # 47
A company's Snowflake account has multiple roles. Each role should have access only to data that resides in the given role's specific region.
When creating a row access policy, which code snippet below will provide privileges to the role ALL_ACCESS_ROLE to see all rows regardless of region, while the other roles can only see rows for their own regions?

- A. create or replace row access policy region policy as (region_value varchar) returns boolean -> exists (select 1 from entitlement_table where role = current_role () and region = region_value)
- B. create or replace row access policy region policy as (region_value varchar) returns boolean ->
  'ALL ACCESS ROLE' = current_role ()
)
- C. create or replace row access policy region policy as (region_value varchar) returns boolean ->
  'ALL_ACCESS_ROLE' = current_role ()
  or exists (
  select 1 from entitlement_table
  where role = current_role ()
  and region = region_value

)

- D. create or replace row access policy region policy as (region_value varchar) returns boolean ->
'ALL ACCESS_ROLE' = current_role ()
and exists (
select 1 from entitlement_table
where role = current_role ()
and region = region_value
)

Answer: C

Explanation:
This code snippet will create a row access policy that returns true if the current role is ALL_ACCESS_ROLE or if the current role matches the region value in the entitlement_table. This means that the ALL_ACCESS_ROLE can see all rows regardless of region, while the other roles can only see rows for their own regions. According to the Snowflake documentation, the CURRENT_ROLE context function returns the name of the current role for the session. The EXISTS function returns true if the subquery returns any rows. The OR operator returns true if either operand is true. Therefore, this code snippet satisfies the requirements of the question.

NEW QUESTION # 48
.....

By adhering to the principle of "quality first, customer foremost", and "mutual development and benefit", our company will provide first class service for our customers. The exam prepare materials of Itcertking is high quality and high pass rate, it is completed by our experts who have a good understanding of Real ADA-C01 Exam and have many years of experience writing study materials. They know very well what candidates really need most when they prepare for the ADA-C01 exam. They also understand the real exam situation very well. We will let you know what a real exam is like.