DS0-001 Q&As

CompTIA DataSys+

Pass CompTIA DS0-001 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/ds0-001.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

Which of the following constraints is used to enforce referential integrity?

A. Surrogate key

B. Foreign key

C. Unique key

D. Primary key

Correct Answer: B

The constraint that is used to enforce referential integrity is foreign key. A foreign key is a column or a set of columns in a table that references the primary key of another table. A primary key is a column or a set of columns in a table that uniquely identifies each row in the table. Referential integrity is a rule that ensures that the values in the foreign key column match the values in the primary key column of the referenced table. Referential integrity helps maintain the consistency and accuracy of the data across related tables. The other options are either different types of constraints or not related to referential integrity at all. For example, a surrogate key is a column that is artificially generated to serve as a primary key, such as an auto-increment number or a GUID (Globally Unique Identifier); a unique key is a column or a set of columns in a table that uniquely identifies each row in the table, but it can have null valuesunlike a primary key; there is no such constraint as TID. References: CompTIA DataSys+ Course Outline, Domain 1.0 Database Fundamentals, Objective 1.2 Given a scenario, execute database tasks using scripting and programming languages.

QUESTION 2

A database administrator would like to create a table named XYZ. Which of the following queries should the database administrator use to create the table?

A)

```
Create Table XYZ(
column1 datatype;
colum2 datatype);
```

B)

```
Create Table XYZ(
column1 datatype,
colum2 datatype);
```

C)

```
Select Table XYZ(
column1 datatype,
colum2 datatype);
```

D)

```
Append Table XYZ(
column1 datatype;
colum2 datatype);
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: B

The query that the administrator should use to create the table is option B. This query uses the CREATE TABLE statement to define a new table named XYZ with three columns: ID, Name, and Age. Each column has a data type and a constraint, such as NOT NULL, PRIMARY KEY, or CHECK. The other options either have syntax errors, use incorrect keywords, or do not specify the table name or columns correctly. References: CompTIA DataSys+ Course Outline, Domain

1.0 Database Fundamentals, Objective 1.1 Given a scenario, identify and apply database structure types.

QUESTION 3

Which of the following resources is the best way to lock rows in SQL Server?

A. TID

B. SID

C. RID

D. PID

Correct Answer: C

The resource that is the best way to lock rows in SQL Server is RID. RID, or Row IDentifier, is an attribute that uniquely identifies each row in a heap table in SQL Server. A heap table is a table that does not have a clustered index, which means that the rows are not stored in any particular order. A RID consists of the file number, page number, and slot number of the row in the database. A RID can be used to lock rows in SQL Server to prevent concurrent access or modification by other transactions or users. A RID lock is a type of lock that locks a single row using its RID. A RID lock can be applied using the HOLDLOCK or XLOCK hints in a SELECT statement. The other options are either not related or not effective for this purpose. For example, TID, or Transaction IDentifier, is an attribute that uniquely identifies each transaction in a database; SID, or Security IDentifier, is an attribute that uniquely identifies each user or group in a Windows system; PID, or Process IDentifier, is an attribute that uniquely identifies each process in an operating system. References: CompTIA DataSys+ Course Outline, Domain 3.0 Database Management and Maintenance, Objective 3.3 Given a scenario, implement database concurrency methods.

QUESTION 4

Which of the following ismostlikely to prevent tampering with server hardware that houses data?

A. Biometric locks

B. Strong password policy

C. Network firewall

D. Surveillance cameras

Correct Answer: A

The option that is most likely to prevent tampering with server hardware that houses data is biometric locks. Biometric locks are devices that use biological characteristics, such as fingerprints, facial recognition, iris scan, etc., to control access to a physical location or resource. Biometric locks help prevent tampering with server hardware that houses data by restricting unauthorized entry or theft of the hardware by intruders or attackers. Biometric locks also provide higher security and convenience than other types of locks, such as keys or passwords, which can be lost, stolen, or forgotten. The other options are either not related or not effective for this purpose. For example, a strong password policy is a set of rules or standards for creating and managing passwords for user accounts or systems; a network firewall is a device or software that controls the incoming and outgoing traffic on a network based on a set of rules or policies; surveillance cameras are devices that capture and record video footage of a physical location or resource. References: CompTIA DataSys+ Course Outline, Domain 4.0 Data and Database Security, Objective 4.2 Given a scenario, implement security controls for databases.

QUESTION 5

A database administrator manages a database server that is running low on disk space. A lot of backup files are stored on the server\\'s disks.

Which of the following is thebestaction for the administrator to take?

A. Move all the backup files to external disks.

B. Delete all the backup files containing data that is rated as classified.

C. Delete all the backup files that are not required by the backup retention policy.

D. Delete all the backup files except for the most recent one.

Correct Answer: C

The best action for the administrator to take is to delete all the backup files that are not required by the backup retention policy. This will free up disk space on the server and also comply with the best practices for data backup and recovery. The backup retention policy defines how long the backup files should be kept and when they should be deleted or archived. The other options are either risky, inefficient, or impractical. For example, moving all the backup files to external disks would require additional hardware and time, deleting all the backup files containing data that is rated as classified would compromise data security and compliance, and deleting all the backup files except for the most recent one would limit the recovery options in case of a disaster. References: CompTIA DataSys+ Course Outline, Domain 5.0 Business Continuity, Objective 5.2 Given a scenario, implement backup and restoration of database management systems.