DS0-001$^{\text{Q\&As}}$

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 statements contains an error?

A. Select EmpId from employee where EmpId=90030

B. Select EmpId where EmpId=90030 and DeptId=34

C. Select* from employee where EmpId=90030

D. Select EmpId from employee

Correct Answer: B

The statement that contains an error is option B. This statement is missing the FROM clause, which specifies the table or tables from which to retrieve data. The FROM clause is a mandatory clause in a SELECT statement, unless the

statement uses a subquery or a set operator. The correct syntax for option B would be:

SELECT EmpId FROM employee WHERE EmpId=90030 AND DeptId=34 Copy

The other options are either correct or valid SQL statements. For example, option A selects the employee ID from the employee table where the employee ID is equal to 90030; option C selects all columns from the employee table where the

employee ID is equal to 90030; option D selects the employee ID from the employee table without any filter condition. 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

An on-premises application server connects to a database in the cloud. Which of the following must be considered to ensure data integrity during transmission?

A. Bandwidth

B. Encryption

C. Redundancy

D. Masking

Correct Answer: B

The factor that must be considered to ensure data integrity during transmission is encryption. Encryption is a process that transforms data into an unreadable or scrambled form using an algorithm and a key. Encryption helps protect data integrity during transmission by preventing unauthorized access or modification of data by third parties, such as hackers, eavesdroppers, or interceptors. Encryption also helps verify the identity and authenticity of the source and destination of the data using digital signatures or certificates. The other options are either not related or not sufficient for this purpose. For example, bandwidth is the amount of data that can be transmitted over a network in a given time; redundancy is the duplication of data or components to provide backup or alternative sources in case of failure; masking is a technique that replaces sensitive data with fictitious but realistic data to protect its confidentiality orcompliance.

References: CompTIA DataSys+ Course Outline, Domain 4.0 Data and Database Security, Objective 4.2 Given a scenario, implement security controls for databases.

QUESTION 3

Which of the following computer services associates IP network addresses with text-based names in order to facilitate identification and connectivity?

A. LDAP

B. NTP

C. DHCP

D. IDNS

Correct Answer: D

The computer service that associates IP network addresses with text-based names in order to facilitate identification and connectivity is IDNS. IDNS, or Internet Domain Name System (DNS), is a service that translates domain names into IP addresses and vice versa. Domain names are human-readable names that identify websites or devices on the internet, such as www.comptia.org or www.google.com. IP addresses are numerical identifiers that locate websites or devices on the internet, such as 104.18.26.46 or 142.250.72.238. IDNS helps users to access websites or devices using domain names instead of IP addresses, which are easier to remember and type. IDNS also helps administrators to manage websites or devices using domain names instead of IP addresses, which are more flexible and scalable. The other options are either different computer services or not related to IP network addresses or text-based names at all. For example, LDAP, or Lightweight Directory Access Protocol, is a service that provides access to directory information such as users, groups, or devices on a network; NTP, or Network Time Protocol, is a service that synchronizes the clocks of computers or devices on a network; DHCP, or Dynamic Host Configuration Protocol, is a service that assigns IP addresses and other network configuration parameters to computers or devices on a network. References: CompTIA DataSys+ Course Outline, Domain 2.0 Database Deployment, Objective 2.1 Given a scenario, select an appropriate database deployment method.

QUESTION 4

A company is launching a proof-of-concept, cloud-based application. One of the requirements is to select a database engine that will allow administrators to perform quick and simple queries on unstructured data.Which of the following would bebestsuited for this task?

A. MonogoDB

B. MS SQL

C. Oracle

D. Graph database

Correct Answer: A

The best suited database engine for this task is MongoDB. MongoDB is a type of non-relational database that stores data as documents in JSON-like format. MongoDB allows administrators to perform quick and simple queries on unstructured data, such as text, images, videos, or social media posts, without requiring a predefined schema or complex joins. MongoDB also supports cloud-based deployment, scalability, and high availability. The other options are either relational databases that require a fixed schema and structure for data, or specialized databases that are designed for specific purposes, such as graph databases for storing and analyzing network data. References: CompTIA DataSys+ Course Outline, Domain 1.0 Database Fundamentals, Objective 1.1 Given a scenario, identify and apply database structure types.

QUESTION 5

Which of the following is used to hide data in a database so the data can only be read by a user who has a key?

A. Data security

B. Data masking

C. Data protection

D. Data encryption

Correct Answer: D

The option that is used to hide data in a database so the data can only be read by a user who has a key is data encryption. Data encryption is a process that transforms data into an unreadable or scrambled form using an algorithm and a key. Data encryption helps protect data from unauthorized access or modification by third parties, such as hackers, eavesdroppers, or interceptors. Data encryption also helps verify the identity and authenticity of the source and destination of the data using digital signatures or certificates. Data encryption can be applied to data at rest (stored in a database) or data in transit (transmitted over a network). To read encrypted data, a user needs to have the corresponding key to decrypt or restore the data to its original form. The other options are either different concepts or not related to hiding data at all. For example, data security is a broad term that encompasses various methods and techniques to protect data from threats or risks; data masking is a technique that replaces sensitive data with fictitious but realistic data to protect its confidentiality or compliance; data protection is a term that refers to the legal or ethical obligations to safeguard personal or sensitive data from misuse or harm. References: CompTIA DataSys+ Course Outline, Domain 4.0 Data and Database Security, Objective 4.2 Given a scenario, implement security controls for databases.