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.pass4itsure.com/ds0-001.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which of the following sets the age requirement for data that should be recovered after a major disaster?

A. MTBF

B. RTO

C. MTTF

D. RPO

Correct Answer: D

The option that sets the age requirement for data that should be recovered after a major disaster is RPO. RPO, or Recovery Point Objective, is a metric that defines the maximum amount of data that can be lost or acceptable data loss in the event of a disaster or disruption. RPOindicates how frequently the data should be backed up or replicated to minimize the risk of data loss. RPO also sets the age requirement for data that should be recovered after a major disaster, as it determines how far back in time the recovery process should go. For example, if the RPO is one hour, then the data should be backed up or replicated every hour, and the recovery process should restore the data to the state it was in one hour before the disaster. The other options are either different metrics or not related to data recovery at all. For example, MTBF, or Mean Time Between Failures, is a metric that measures the average time that a system or component operates without failure; RTO, or Recovery Time Objective, is a metric that defines the maximum amount of time that can be taken to restore a system or service after a disaster or disruption; MTTF, or Mean Time To Failure, is a metric that measures the average time that a system or component operates until it fails. References: CompTIA DataSys+ Course Outline, Domain 5.0 Business Continuity, Objective 5.3 Given a scenario, implement backup and restoration of data.

QUESTION 2

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 3

Which of the following is an attack in which an attacker hopes to profit from locking the database software?

A. Spear phishing

B. Ransomware

C. SQL injection

D. On-path

Correct Answer: B

The attack in which an attacker hopes to profit from locking the database software is ransomware. Ransomware is a type of malware that encrypts the data or files on a system or network and demands a ransom from the victim to restore them. Ransomware can target database software and lock its access or functionality until the victim pays the ransom, usually in cryptocurrency. Ransomware can cause serious damage and loss to the victim, as well as expose them to further risks or threats. Ransomware can be delivered through various methods, such as phishing emails, malicious attachments, compromised websites, etc. The other options are either different types of attacks or not related to locking database software at all. For example, spear phishing is a type of phishing attack that targets a specific individual or organization with personalized or customized emails; SQL injection is a type of attack that inserts malicious SQL statements into an input field or parameter of a web application to manipulate or compromise the underlying database; on-path is a type of attack that intercepts and modifies the data in transit between two parties on a network. References: CompTIA DataSys+ Course Outline, Domain 4.0 Data and Database Security, Objective 4.4 Given a scenario, identify common types of attacks against databases

QUESTION 4

Which of the following indexes stores records in a tabular format?

A. Columnstore

B. Non-clustered

C. Unique

D. Secondary

Correct Answer: A

The index that stores records in a tabular format is columnstore. A columnstore index is a type of index that stores and compresses data by columns rather than by rows. A columnstore index can improve the performance and efficiency of queries that perform aggregations, calculations, or analysis on large amounts of data, such as data warehouse or business intelligence applications. A columnstore index can also reduce the storage space required for data by applying various compression techniques, such as dictionary encoding, run-length encoding, bit packing, etc. The other options are either different types of indexes or not related to indexes at all. For example, a non-clustered index is a type of index that stores the values of one or more columns in a sorted order along with pointers to the corresponding rows in the table; a unique index is a type of index that enforces uniqueness on one or more columns in a table; a secondary index is an alternative term for a non-clustered index. References: CompTIA DataSys+ Course Outline, Domain 3.0 Database Management and Maintenance, Objective 3.1 Given a scenario, perform common database maintenance tasks.

QUESTION 5

Which of the following services is responsible for assigning, managing, and reclaiming IP addresses on a TCP/IP-based network?

A. DNS

B. DHCP

C. LDAP

D. ISMTP

Correct Answer: B

The service that is responsible for assigning, managing, and reclaiming IP addresses on a TCP/IP-based network is DHCP. DHCP, or Dynamic Host Configuration Protocol, is a service that automatically assigns IP addresses and other network configuration parameters, such as subnet mask, default gateway, DNS server, etc., to computers or devices on a network. DHCP helps simplify the administration and management of IP addresses on a network, as well as avoid conflicts or errors caused by manual or duplicate assignments. DHCP also allows computers or devices to release or renew their IP addresses when they join or leave the network. The other options are either different services or not related to IP addresses at all. For example, DNS, or Domain Name System, is a service that translates domain names into IP addresses and vice versa; LDAP, or Lightweight Directory Access Protocol, is a service that provides access to directory information such as users, groups, or devices on a network; ISMTP is not a valid acronym or service. References: CompTIA DataSys+ Course Outline, Domain 2.0 Database Deployment, Objective 2.1 Given a scenario, select an appropriate database deployment method.