CLO-002 Q&As

CompTIA Cloud Essentials+

QUESTION 1

Which of the following describes the process of moving an application from an isolated data center to reduce latency and ensure close proximity to end users?

A. Replication

B. Zones

C. Geo-redundancy

D. Backup

Correct Answer: C

Explanation: Geo-redundancy is the distribution of mission-critical components or infrastructures, such as servers, across multiple data centers that reside in different geographic locations1. Geo-redundancy acts as a safety net in case the primary site fails or in the event of a disaster or an outage that impacts an entire region1. Geo-redundancy also reduces latency and ensures close proximity to end users by delivering web content from the nearest data center2. Geo-redundancy is a common feature of cloud computing, as it provides high availability, reliability, and performance for cloud applications and services2. Replication is the process of copying data from one location to another, such as from a primary site to a secondary site, or from one cloud provider to another3. Replication is a necessary but not sufficient condition for geo-redundancy, as it does not guarantee that the replicated data is accessible or consistent across different regions3. Replication can also introduce operational complexity and data synchronization issues3. Zones are logical or physical partitions of a cloud provider\\'s infrastructure that offer high availability and fault tolerance within a region4. Zones are usually located in the same or nearby data centers, and are connected by low-latency network links4. Zones can help distribute the workload and prevent single points of failure, but they do not provide geo-redundancy, as they are still vulnerable to regional outages or disasters4. Backup is the process of creating and storing copies of data for the purpose of recovery in case of data loss or corruption5. Backup is an important part of data protection and disaster recovery, but it does not provide geo-redundancy, as it does not ensure that the backup data is available or up-to-date in different regions5. Backup can also have longer recovery time and higher cost than geo-redundancy5. References: Use georedundancy to design highly available applications; Geo Redundancy Explained | Cloudify; Georedundancy - Open Telekom Cloud; Why geo-redundancy for cloud infrastructure is a `must have\\'; Geo-Redundancy: Why Is It So Important? | Unitrends.

QUESTION 2

A contract that defines the quality and performance metrics that are agreeable to both parties is called an:

A. SOP.

B. SOA.

C. SOW.

D. SLA.

Correct Answer: D

Explanation: A service level agreement (SLA) is a contract that defines the quality and performance metrics that are agreeable to both parties. An SLA specifies the expectations and responsibilities of the service provider and the customer in terms of service availability, reliability, security, and responsiveness. An SLA also defines the penalties or remedies for non-compliance with the agreed-upon metrics. An SLA is a key component of cloud computing contracts, as it ensures that the cloud service provider delivers the service according to the customer\\'s requirements and expectations12. References: CompTIA Cloud Essentials+ CLO-002 Study Guide, Chapter 3: Cloud Business Principles, Section 3.4: Cloud Service Agreements, p. 117-1181 What is SLA? - Service Level Agreement Explained - AWS 2

QUESTION 3

Which of the following is a scientific study of algorithms and statistical models that a computer system integrates to improve performance of a specific task effectively based on information?

A. IoT

B. Big Data

C. Machine learning

D. Blockchain

Correct Answer: C

Explanation: Machine learning Comprehensive Explanation: Machine learning is a scientific study of algorithms and statistical models that a computer system integrates to improve performance of a specific task effectively based on information1. Machine learning is a subfield of artificial intelligence that uses data and algorithms to imitate the way that humans learn, gradually improving its accuracy2. Machine learning enables machines to perform tasks that would otherwise only be possible for humans, such as categorizing images, analyzing data, or predicting price fluctuations2. Machine learning algorithms are typically created using frameworks that accelerate solution development, such as TensorFlow and PyTorch2. IoT, or Internet of Things, is a network of physical devices, vehicles, appliances, and other items embedded with sensors, software, and connectivity that enable these objects to exchange data and interact with each other3. IoT is not a scientific study of algorithms and statistical models, but a technological paradigm that connects various devices and systems to the internet. Big Data is a term that refers to the large, complex, and diverse sets of data that are generated at high speed from various sources, such as social media, sensors, web logs, or transactions4. Big Data is not a scientific study of algorithms and statistical models, but a data phenomenon that poses challenges and opportunities for analysis and processing. Blockchain is a system of storing and transferring information in a distributed, decentralized, and secure way using cryptographic principles and peer-to-peer networks5. Blockchain is not a scientific study of algorithms and statistical models, but a data structure and protocol that enables trustless and transparent transactions and records. References : Machine learning -Wikipedia; What Is Machine Learning? Definition, Types, and Examples; What is the Internet of Things (IoT)? | IBM; What is big data? | IBM; What is blockchain? | IBM.

QUESTION 4

A business analyst has been drafting a risk response for a vulnerability that was identified on a server. After considering the options, the analyst decides to decommission the server. Which of the following describes this approach?

A. Mitigation

B. Transference

C. Acceptance

D. Avoidance

Correct Answer: D

Explanation: Avoidance is a risk response strategy that involves eliminating the threat or uncertainty associated with a risk by removing the cause or the source of the risk. Avoidance can help to prevent the occurrence or the impact of a negative risk, but it may also result in the loss of potential opportunities or benefits. Avoidance is usually applied when the risk is too high or too costly to mitigate, transfer, or accept12 The business analyst is using the avoidance strategy by decommissioning the server that has a vulnerability. By doing so, the analyst is eliminating the possibility of the vulnerability being exploited or causing harm to the system or the data. However, the analyst is also losing the functionality or the value that the server provides, and may need to find an alternative solution or resource. Mitigation is not the correct answer, because mitigation is a risk response strategy that involves reducing the probability or the impact of a negative risk by implementing actions or controls that can minimize or counteract the risk. Mitigation can help to lower the exposure or the severity of a risk, but it does not eliminate the risk completely. Mitigation is usually applied when the risk is moderate or manageable, and the cost of mitigation is justified by the potential benefit12 Transference is not the correct answer, because transference is a risk response strategy that involves shifting the responsibility or the impact of a negative risk to a third party, such as a vendor, a partner, or an insurer. Transference can help to share or distribute the risk, but it does not reduce or remove the risk. Transference is usually applied when the risk is beyond the control or the expertise of the organization, and the cost of transference is acceptable or affordable12 Acceptance is not the correct answer, because acceptance is a risk response strategy that involves acknowledging the existence or the possibility of a negative risk, and being prepared to deal with the consequences if the risk occurs. Acceptance can be passive, which means no action is taken to address the risk, or active, which means a contingency plan or a reserve is established to handle the risk. Acceptance is usually applied when the risk is low or inevitable, and the cost of avoidance, mitigation, or transference is higher than the cost of acceptance12 References: 1: https://www.projectengineer.net/5-risk-response-strategies/ 2: https://www.comptia.org/training/books/cloud-essentials-clo-002-study-guide, page 50

QUESTION 5

Which of the following is a security advantage of using CDNs?

A. Advanced threat inspection

B. VPN sessions to the consumers

C. Resiliency against DDoS attacks

D. Data encryption at rest

Correct Answer: C

Explanation: A content delivery network (CDN) is a network of servers that deliver web content to users based on their geographic location. A CDN can improve the performance, reliability, and security of a web application by caching content closer to the users and reducing the load on the origin server. One of the security advantages of using a CDN is that it can provide resiliency against distributed denial-of-service (DDoS) attacks, which are attempts to overwhelm a web server with a large number of requests from multiple sources. A CDN can mitigate DDoS attacks by: Distributing the traffic across multiple servers and locations, making it harder for attackers to target a single point of failure Filtering out malicious requests before they reach the origin server, using techniques such as rate limiting, IP blocking, and challenge-response mechanisms Absorbing the attack traffic with greater bandwidth and resources than the origin server, reducing the impact on the web application\\'s availability and performance References: CompTIA Cloud Essentials+ CLO-002 Study Guide, Chapter 4: Security in the Cloud, page 152; Why use a CDN? | CDN benefits | Cloudflare; What Is DNS Security? How Does It Work? - Cisco Umbrella; What is DNS Security? - Cisco Umbrella; What Is DNS Security? DNS vs DNS Security vs DNSSEC | Fortinet

Latest CLO-002 Dumps CLO-002 Practice Test CLO-002 Study Guide