



CLO-002^{Q&As}

CompTIA Cloud Essentials+

Pass CompTIA CLO-002 Exam with 100% Guarantee

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

<https://www.passapply.com/clo-002.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 is achieved by implementing replication, redundancy, and disaster recovery?

- A. Improved performance
- B. Improved throughput
- C. Improved latency
- D. Improved availability

Correct Answer: D

Explanation: Availability is the degree to which a system or service is accessible and functional when required. Availability can be measured by metrics such as uptime, downtime, and service level agreements (SLAs). Availability can be improved by implementing replication, redundancy, and disaster recovery strategies in the cloud. Replication is the process of creating and maintaining multiple copies of data or resources across different locations or regions. Redundancy is the provision of extra or backup components or systems to prevent or mitigate failures. Disaster recovery is the ability to restore normal operations after a disruptive event, such as a natural disaster, a cyberattack, or a human error. By implementing these strategies, cloud users can ensure that their data and services are always accessible and resilient to failures or disasters. References: CompTIA Cloud Essentials+ CLO-002 Study Guide, page 103- 104; CompTIA Cloud+ (Plus) Certification

QUESTION 2

A company has decided to replicate cloud resources in several different geographic locations. Which of the following terms BEST describes this approach?

- A. Disaster recovery
- B. Deduplication
- C. Redundancy
- D. Data sovereignty

Correct Answer: C

Explanation: Redundancy is a term that describes the approach of replicating cloud resources in several different geographic locations. Redundancy can increase the availability, reliability, and performance of cloud services by providing backup or alternative resources in case of failures, disasters, or high demand. Redundancy can also reduce latency by serving users from the nearest location. Redundancy can be implemented at different levels, such as data, network, server, or application. For example, a geo- distributed database is a type of redundancy that offers asynchronous replication across two data centers or cloud regions¹. Redundancy is different from disaster recovery, deduplication, and data sovereignty, which are other terms related to cloud computing. Disaster recovery is a term that describes the process of restoring normal operations after a disaster or disruption. Disaster recovery can involve using redundant resources, but it is not the same as redundancy. Deduplication is a term that describes the technique of eliminating redundant copies of data from a storage device, which can reduce the storage space required and improve the efficiency of the storage system. Deduplication does not involve replicating cloud resources in different locations, but rather consolidating and removing duplicates. Data sovereignty is a term that describes the legal and regulatory aspects of data storage and processing in different geographic locations. Data sovereignty can affect the choice of cloud regions and providers, as some countries or regions may have specific laws or regulations that govern the access, transfer, and



protection of data. Data sovereignty does not imply redundancy, but rather compliance. Therefore, the correct term for replicating cloud resources in several different geographic locations is redundancy. References: Geography and regions | Documentation | Google Cloud, What is Database Geo-Distribution? - Yugabyte, Georedundancy: geographical redundancy | StackScale.

QUESTION 3

An analyst is reviewing a report on a company's cloud resources expenditures. The analyst has noted that a data warehouse team uses a significant amount of high-speed storage for live databases and backups. Which of the following should the analyst recommend for improved cost and efficiency?

- A. Configure the live database for redundant clustering.
- B. Move the backups to slower storage.
- C. Configure geo-redundancy for backups.
- D. Move the backups to another availability zone.

Correct Answer: B

Explanation: High-speed storage, such as solid-state drives (SSDs), is more expensive and faster than slower storage, such as hard disk drives (HDDs). High-speed storage is suitable for live databases that require low latency and high performance, but not for backups that are rarely accessed and do not need fast retrieval. Therefore, the analyst should recommend moving the backups to slower storage, which can reduce the cost and improve the efficiency of the cloud resources expenditures. Moving the backups to slower storage can also free up more space for the live database on the high-speed storage¹. Configuring the live database for redundant clustering, configuring geo-redundancy for backups, or moving the backups to another availability zone are not recommended for improved cost and efficiency, as they would increase the complexity and expense of the cloud resources. Redundant clustering and geo-redundancy are techniques for enhancing the availability and reliability of the data, but they also require more storage and network resources². Moving the backups to another availability zone may improve the fault tolerance and latency of the backups, but it may also incur additional fees for data transfer and storage³. References: Choose between SSD and HDD storage - Google Cloud; Cloud Computing vs. Cloud Storage | Pure Storage; Cloud Storage vs. Local Storage | Enterprise Storage Forum.

QUESTION 4

A cloud systems administrator needs to migrate several corporate applications to a public cloud provider and decommission the internal hosting environment. This migration must be completed by the end of the month. Because these applications are internally developed to meet specific business accounting needs, the administrator cannot use an alternative application.

Which of the following BEST describes the approach the administrator should use?

- A. Hybrid deployment
- B. Phased migration
- C. Lift and shift
- D. Rip and replace

Correct Answer: C



Explanation: Lift and shift is a cloud migration strategy that involves moving an application or workload from one environment to another without making significant changes to its architecture, configuration, or code. This approach is suitable for applications that are not cloud-native, have complex dependencies, or have tight deadlines for migration. Lift and shift can help reduce the cost and risk of maintaining legacy infrastructure, improve scalability and availability, and leverage cloud services and features¹². Hybrid deployment is a cloud deployment model that involves using both public and private cloud resources to deliver services and applications. This approach is suitable for applications that have varying performance, security, or compliance requirements, or that need to integrate with existing on-premises systems. Hybrid deployment can help optimize the use of resources, increase flexibility and agility, and balance trade-offs between cost and control³⁴. Phased migration is a cloud migration strategy that involves moving an application or workload from one environment to another in stages or increments. This approach is suitable for applications that have modular components, low interdependencies, or high complexity. Phased migration can help reduce the impact of migration on business operations, test the functionality and performance of each component, and address any issues or challenges along the way . Rip and replace is a cloud migration strategy that involves discarding an application or workload from one environment and replacing it with a new one in another environment. This approach is suitable for applications that are outdated, incompatible, or inefficient, or that have high maintenance costs. Rip and replace can help modernize the application architecture, design, and code, improve the user experience and functionality, and take advantage of cloud-native features and services . References: [CompTIA Cloud Essentials+ CLO-002 Study Guide], Chapter 3: Management and Technical Operations, Section 3.3: Cloud Migration, p. 123-125 [CompTIA Cloud+ CV0-003 Study Guide], Chapter 5: Deploying a Cloud Solution, Section 5.2: Cloud Migration, p. 241-244 [CompTIA Cloud Essentials+ CLO-002 Study Guide], Chapter 1: Cloud Concepts, Section 1.3: Cloud Deployment Models, p. 25-28 [CompTIA Cloud+ CV0-003 Study Guide], Chapter 1: Cloud Architecture and Design, Section 1.2: Cloud Deployment Models, p. 19-22 [CompTIA Cloud Essentials+ CLO-002 Study Guide], Chapter 3: Management and Technical Operations, Section 3.3: Cloud Migration, p. 125-126 [CompTIA Cloud+ CV0-003 Study Guide], Chapter 5: Deploying a Cloud Solution, Section 5.2: Cloud Migration, p. 244-245 [CompTIA Cloud Essentials+ CLO-002 Study Guide], Chapter 3: Management and Technical Operations, Section 3.3: Cloud Migration, p. 126-127 [CompTIA Cloud+ CV0-003 Study Guide], Chapter 5: Deploying a Cloud Solution, Section 5.2: Cloud Migration, p. 245-246 [CompTIA Cloud Essentials+ CLO-002 Study Guide], ISBN: 978-1-119-64768-9, Publisher: Wiley [CompTIA Cloud+ CV0-003 Study Guide], ISBN: 978-1-119-64767-2, Publisher: Wiley

QUESTION 5

Which of the following are considered secure access types of hosts in the cloud? (Choose two.)

- A. HTTPS
- B. HTTP
- C. SSH
- D. Telnet
- E. RDP
- F. FTP

Correct Answer: AC

Explanation: HTTPS and SSH are considered secure access types of hosts in the cloud because they use encryption and authentication to protect the data and the identity of the users. HTTPS is a protocol that uses SSL or TLS to encrypt the

communication between a web browser and a web server. SSH is a protocol that allows secure remote login and file transfer over a network. Both HTTPS and SSH prevent unauthorized access, eavesdropping, and tampering of the data in



transit. References: CompTIA Cloud Essentials+ Certification Study Guide, Second Edition (LO-002), Chapter 3: Security in the Cloud, pages 83-84.

[Latest CLO-002 Dumps](#)

[CLO-002 VCE Dumps](#)

[CLO-002 Study Guide](#)