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

D. A password that expires after 90 days and a PIN

Correct Answer: B

Explanation: Multifactor authentication (MFA) is a method of verifying a user\\'s identity by requiring more than one factor, such as something the user knows, something the user has, or something the user is1. A short message service (SMS) message sent to a phone and an access PIN is an example of MFA, as it combines two factors: something the user has (the phone) and something the user knows (the PIN). This makes the authentication process more secure than using only a password, which is a single factor. Other examples of MFA include using a biometric scan (such as a fingerprint or a face recognition) and a password, or using a hardware token (such as a smart card or a USB key) and a password1. References: 1: CompTIA Cloud Essentials+ Certification Study Guide, Second Edition (LO-002), Chapter 3: Cloud Planning, Section 3.2: Cloud Adoption, Subsection 3.2.1: Identity and Access Management

QUESTION 2

A company deploys a data management capability that reduces RPO. Which of the following BEST describes the capability needed?

A. Locality

B. Replication

C. Portability

D. Archiving

Correct Answer: B

Explanation: Replication is a data management capability that involves creating and maintaining copies of data across multiple locations or systems1. Replication can help reduce the Recovery Point Objective (RPO) of an application, which is the maximum acceptable amount of data loss measured in time2. By replicating data frequently and consistently, the risk of losing data in the event of a disruption or failure is minimized, as the data can be restored from the most recent replica. Replication can also improve the availability, performance, and scalability of an application, as the data can be accessed from multiple sources and distributed across different regions3. Locality is a data management capability that refers to the physical location or proximity of data to the users or applications that access it4. Locality can affect the latency, bandwidth, and cost of data transfer, as well as the compliance with data sovereignty and privacy regulations. Locality does not directly reduce the RPO of an application, but rather influences the choice of where to store and replicate data. Portability is a data management capability that refers to the ease of moving data across different platforms, systems, or environments. Portability can enable the interoperability, integration, and migration of data, as well as the flexibility and agility of data management. Portability does not directly reduce the RPO of an application, but rather enables the use of different data sources and destinations. Archiving is a data management capability that involves moving or copying data that is no longer actively used to a separate storage device or system for long-term retention. Archiving can help optimize the storage space, performance, and cost of data, as well as comply with data retention and preservation policies. Archiving does not directly reduce the RPO of an application, but rather preserves the historical data for future reference or analysis. References: CompTIA Cloud Essentials+ CLO-002 Study Guide, Chapter 3: Cloud Data Management, pages 97-99.

QUESTION 3

Which of the following BEST specifies how software components interoperate in a cloud environment?

A. Federation

B. Regression

C. Orchestration

D. API integration

Correct Answer: B

Explanation: A disaster recovery plan (DRP) is a document that defines the procedures and resources needed to restore normal operations after a major disruption. A DRP typically includes the following elements: The scope and objectives of the plan The roles and responsibilities of the DR team The inventory and location of critical assets and resources The recovery strategies and procedures for different scenarios The testing and maintenance schedule for the plan The communication plan for internal and external stakeholders One of the key components of a DRP is the recovery sequence, which is the optimal, sequential order in which cloud resources should be recovered in the event of a major failure. The recovery sequence is based on the priority and dependency of the resources, as well as the recovery time objective (RTO) and recovery point objective (RPO) of the business. The recovery sequence helps to minimize the downtime and data loss, and ensure the continuity of the business operations. A recovery point objective (RPO) is the maximum acceptable amount of data loss measured in time. It indicates how often the data should be backed up and how much data can be restored after a disaster. A recovery time objective (RTO) is the maximum acceptable amount of time that a system or application can be offline after a disaster. It indicates how quickly the system or application should be restored and how much downtime can be tolerated by the business. An incident response plan (IRP) is a document that defines the procedures and actions to be taken in response to a security breach or cyberattack. An IRP typically includes the following elements: The scope and objectives of the plan The roles and responsibilities of the incident response team The incident identification and classification criteria The incident containment, eradication, and recovery steps The incident analysis and reporting methods The incident prevention and improvement measures A network topology diagram is a visual representation of the physical and logical layout of a network. It shows the devices, connections, and configurations of the network. A network topology diagram can help to identify the potential points of failure, the impact of a failure, and the recovery options for a network. However, it does not define the optimal, sequential order in which cloud resources should be recovered in the event of a major failure. References: The following sources were used to create this answer: Disaster recovery planning guide | Cloud Architecture Center - Google Cloud What is Disaster Recovery and Why Is It Important? - Google Cloud Key considerations when building a disaster recovery plan for private cloud - Continuity Central 12 Essential Points Of the Disaster Recovery Plan Checklist - NAKIVO Building a Cloud Disaster Recovery Plan: Tips and Approaches - MSP360

QUESTION 4

Which of the following allows an IP address to be referenced via an easily remembered name for a SaaS application?

A. DNS

B. CDN

C. VPN

D. WAN

Correct Answer: A

Explanation: DNS stands for Domain Name System, which is a service that translates domain names into IP addresses.

Domain names are easier to remember than IP addresses, and they can also change without affecting the users. For

example, a SaaS application can have a domain name like www.saas.com, which can be resolved to different IP addresses depending on the location, availability, and performance of the servers. DNS allows users to access the SaaS

application by typing the domain name in their browser, instead of memorizing the IP address. References:

https://www.comptia.org/training/books/cloud-essentials-clo-002-study-guide, Chapter 2, page 43.

QUESTION 5

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.