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.pass2lead.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

A cloud developer chooses to use private key encryption for all traffic in a new application. Which of the following security concerns does this BEST describe?

A. Integrity

B. Confidentiality

C. Availability

D. Authorization

Correct Answer: B

Explanation: Private key encryption, also known as symmetric key encryption, is a method of encrypting data using a single secret key that is shared by both the sender and the receiver of the message1. Private key encryption ensures that only the authorized parties who have the same key can access the encrypted data, while preventing unauthorized parties from reading or modifying it. Therefore, private key encryption is mainly used to protect the confidentiality of data, which is the security concern that deals with preventing unauthorized disclosure of information2. Confidentiality is one of the three main goals of information security, along with integrity and availability. Integrity refers to the security concern that deals with preventing unauthorized modification or corruption of information. Availability refers to the security concern that deals with ensuring timely and reliable access to information2. Authorization, on the other hand, is not a security concern, but a security mechanism that deals with granting or denying access rights to information based on predefined policies and rules3. A cloud developer chooses to use private key encryption for all traffic in a new application. This best describes the security concern of confidentiality, as the developer wants to ensure that only the intended recipients can access the encrypted data, while keeping it secret from anyone else. References: 1: https://www.comptia.org/training/books/cloud-essentials-clo-002-study-guide, Chapter 8, page 274-275 2: https://www.comptia.org/training/books/cloud-essentials-clo-002-study- guide, Chapter 8, page 263-264 3: https://www.comptia.org/ training/books/cloud- essentials-clo-002-study-guide, Chapter 8, page 268-269

QUESTION 2

Which of the following policies dictates when to grant certain read/write permissions?

A. Access control

B. Communications

C. Department-specific

D. Security

Correct Answer: A

Explanation: Access control is a policy that dictates when to grant certain read/write permissions to users or systems. Access control is a key component of information security, as it ensures that only authorized and authenticated users can access the data and resources they need, and prevents unauthorized access or modification of data and resources1. Access control policies can be based on various factors, such as identity, role, location, time, or context2. Communications, department-specific, and security policies are not directly related to granting read/write permissions, although they may have some implications for access control. Communications policies are policies that define how information is exchanged and communicated within or outside an organization, such as the use of email, social media, or encryption3. Department-specific policies are policies that apply to specific functions or units within an organization,

such as human resources, finance, or marketing. Security policies are policies that establish the overall goals and objectives of information security in an organization, such as the protection of confidentiality, integrity, and availability of data and systems. References: Access Control Policy and Implementation Guides | CSRC; What Is Access Control? | Microsoft Security; Communication Policy - Definition, Examples, Cases, Processes; [Departmental Policies and Procedures Manual Template | Policies and Procedures Manual Template]; [Security Policy - an overview | ScienceDirect Topics].

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

A business analyst is drafting a proposal for eliminating redundant copies of data from a SAN disk drive. Which of the following terms should the analyst mention in the proposal?

A. Deduplication

B. Encryption

C. Sanitization

D. Compression

Correct Answer: A

Explanation: Deduplication is a technique that eliminates redundant copies of data from a storage device, such as a SAN disk drive. Deduplication can reduce the amount of storage space required and improve the performance and efficiency of the storage system. Deduplication works by identifying and removing duplicate blocks of data within or across files, and replacing them with pointers to a single copy of the data. Deduplication can be performed at the file level or the block level, depending on the granularity and the algorithm used. Deduplication is often used in backup and archive scenarios, where data is highly redundant and can be deduplicated across multiple backups. Deduplication can also be used in primary storage scenarios, such as SAN disk drives, especially for all-flash arrays that implement deduplication techniques. Deduplication is different from compression, which is another technique that reduces the size of data by removing redundant information within a data block. Deduplication and compression can work together to achieve higher storage savings. Deduplication is also different from encryption, which is a technique that protects the confidentiality and integrity of data by transforming it into an unreadable form using a secret key. Deduplication is not effective for encrypted data, as encryption makes the data appear random and unique. Deduplication is also different from sanitization, which is a technique that permanently erases data from a storage device, making it unrecoverable. Deduplication does not erase data, but rather consolidates it and removes duplicates. Therefore, the correct term for eliminating redundant copies of data from a SAN disk drive is deduplication. References: Using Deduplication and Compression, Understanding Data Deduplication, 7.6 Using Deduplication techniques in SAN infrastrucutre.

QUESTION 5

A business analyst is comparing used vs. allocated storage cost for each reserved instance on a financial expenditures report related to the cloud. The CSP is currently billing at the following rates for storage:

$1.50 per GB of used space $0.75 per GB of allocated space

The operating expenditures the analyst is reviewing are as follows:

Server name	Used space	Allocated space
Application server	18GB	100GB
Mail server	55GB	80GB
File server	70GB	90GB

Given this scenario, which of the following servers is costing the firm the least, and which should have storage increased due to over 70% utilization?

A. Least: File server Optimize: Application server

B. Least: Application server Optimize: Mail server

C. Least: Mail server Optimize: File server

D. Least: Application server Optimize: File server

Correct Answer: D

The least costing server is the application server because it has the lowest used space and allocated space. The file

server should have storage increased due to over 70% utilization because it has the highest used space and allocated

space. To calculate the cost of each server, we can use the following formula:

Cost = ($1.50 x Used space) + ($0.75 x Allocated space) Using this formula, we can find the cost of each server as follows:

Application server: Cost = ($1.50 x 186 GB) + ($0.75 x 250 GB) = $279 + $187.50 = $466.50

Mail server: Cost = ($1.50 x 250 GB) + ($0.75 x 300 GB) = $375 + $225 = $600 File server: Cost = ($1.50 x 450 GB) + ($0.75 x 500 GB) = $675 + $375 = $1050 The application server has the lowest cost of $466.50, while the file server has

the highest cost of $1050. To find the utilization percentage of each server, we can use the following formula:

Utilization = (Used space / Allocated space) x 100% Using this formula, we can find the utilization percentage of each server as follows:

Application server: Utilization = (186 GB / 250 GB) x 100% = 74.4% Mail server: Utilization = (250 GB / 300 GB) x 100% = 83.3% File server: Utilization = (450 GB / 500 GB) x 100% = 90% The file server has the highest utilization percentage

of 90%, which means that it is running out of storage space and may affect its performance and availability. The application server has the lowest utilization percentage of 74.4%, which means that it has some unused storage space and may

be overprovisioned. Therefore, the file server should have storage increased to reduce its utilization and improve its efficiency, while the application server is costing the firm the least and does not need any changes in its storage allocation.

References: CompTIA Cloud Essentials+ CLO-002 Study Guide, Chapter 3: Cloud Business Principles, Section 3.4: Cloud Billing and Cost Management, Page 87 and [Cloud Storage Utilization and Optimization | CloudHealth by VMware]

CLO-002 Practice Test CLO-002 Exam Questions CLO-002 Braindumps