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.pass4itsure.com/clo-002.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

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 2

A company migrated all of its infrastructure to the cloud. The cloud security team must review the security post-migration.

Which of the following is the MOST appropriate task for the cloud security team to perform?

A. Risk register

B. Threat assessment

C. Application scan

D. Vulnerability scan

Correct Answer: D

Explanation: A vulnerability scan is a process of identifying and reporting potential security weaknesses in a system or network. A vulnerability scan can help detect misconfigurations, outdated software, missing patches, and other issues that could compromise the security of the cloud environment. A vulnerability scan is an appropriate task for the cloud security team to perform after migrating the infrastructure to the cloud, as it can help identify and remediate any security gaps that may have occurred during the migration process. A vulnerability scan can also help the cloud security team comply with the security standards and regulations that apply to the cloud service provider and the cloud customer. A risk register is a document that lists the identified risks, their likelihood, impact, and mitigation strategies for a project or organization. A risk register is not a post-migration task, but rather a pre-migration task that should be created and updated throughout the cloud migration process. A risk register can help the cloud security team assess and manage the risks associated with the cloud migration, and plan for contingencies and backups in case of any unforeseen events. A threat assessment is a process of identifying and analyzing the potential threats that could harm a system or network. A threat assessment can help the cloud security team determine the sources, motives, capabilities, and methods of the attackers, and prioritize the most critical and likely threats. A threat assessment is not a post-migration task, but rather a continuous task that should be performed regularly to monitor and respond to the evolving threat landscape. A threat assessment can help the cloud security team enhance the security posture and resilience of the cloud environment, and implement appropriate countermeasures and controls. An application scan is a process of testing and verifying the functionality and security of an application. An application scan can help detect and report any errors, bugs, vulnerabilities, or performance issues in an application. An application scan is not a post-migration task, but rather a development and deployment task that should be performed before and after launching an application in the cloud. An application scan can help the cloud security team ensure the quality and reliability of the application, and fix any issues that could affect the user experience or security of the application. References: CompTIA Cloud Essentials+ CLO-002 Study Guide, Chapter 4: Cloud Security Principles and Practices, pages 153-154.

QUESTION 3

Which of the following cloud migration methods would be BEST suited for disaster recovery scenarios?

A. Replatforming

B. Phased

C. Rip and replace

D. Lift and shift

Correct Answer: D

Explanation: Lift and shift is a cloud migration method that involves moving an application or workload from one environment to another without making any significant changes to its architecture, configuration, or code. Lift and shift is also known as rehosting or forklifting. Lift and shift is best suited for disaster recovery scenarios because it allows for a fast and simple migration of applications or workloads to the cloud in case of a disaster or disruption in the original environment. Lift and shift can also reduce the risk of errors or compatibility issues during the migration process, as the application or workload remains unchanged. Lift and shift can also leverage the cloud\\'s scalability, availability, and security features to improve the performance and resilience of the application or workload. However, lift and shift may not take full advantage of the cloud\\'s native capabilities and services, and may incur higher operational costs due to the maintenance of the legacy infrastructure and software. Therefore, lift and shift may not be the best option for long-term or strategic cloud migration, but rather for short-term or tactical cloud migration for disaster recovery purposes. Replatforming, phased, and rip and replace are not the best cloud migration methods for disaster recovery scenarios, as they involve more changes and complexity to the application or workload, which may increase the migration time and risk. Replatforming is a cloud migration method that involves making some modifications to the application or workload to optimize it for the cloud environment, such as changing the operating system, database, or middleware. Replatforming is also known as replatforming or refactoring. Replatforming can improve the performance and efficiency of the application or workload in the cloud, but it may also introduce some challenges and costs, such as testing, debugging, and licensing. Phased is a cloud migration method that involves moving an application or workload to the cloud in stages or increments, rather than all at once. Phased is also known as iterative or hybrid. Phased can reduce the impact and risk of the migration process, as it allows for testing, feedback, and adjustment along the way. However, phased can also prolong the migration time and effort, as it requires more coordination and integration between the source and target environments. Rip and replace is a cloud migration method that involves discarding the existing application or workload and building a new one from scratch in the cloud, using cloud-native technologies and services. Rip and replace is also known as rebuild or cloud-native. Rip and replace can maximize the benefits and potential of the cloud, but it may also entail the highest cost and complexity, as it requires a complete redesign and redevelopment of the application or workload. References: CompTIA Cloud Essentials+ CLO-002 Study Guide, Chapter 7: Cloud Migration, Section 7.2: Cloud Migration Methods, Page 2111 and Cloud Migration Strategies: A Guide to Moving Your Infrastructure | Rackspace Technology

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

Before conducting a cloud migration, a compliance team requires confirmation that sensitive data will remain close to their users. Which of the following will meet this requirement during the cloud design phase?

A. Data locality

B. Data classification

C. Data certification

D. Data validation

Correct Answer: A

Explanation: Data locality is the principle of storing data close to where it is used, such as in the same region, country, or jurisdiction. Data locality can improve the performance, security, and compliance of cloud applications, especially when dealing with sensitive data that is subject to legal or regulatory requirements. Data locality can also reduce the network latency and bandwidth costs associated with transferring data across long distances. Data locality can be achieved by choosing a cloud provider that has data centers in the desired locations, and by specifying the data placement and migration policies in the cloud design phase. Data locality is different from data classification, data certification, and data validation. Data classification is the process of categorizing data based on its sensitivity, value, and risk. Data certification is the process of verifying that data meets certain standards or criteria. Data validation is the process of checking that data is accurate, complete, and consistent. References: Data Locality - an overview | ScienceDirect Topics, Data Locality: What It Is and Why It Matters - Qumulo, Cloud Computing Design Principles - CompTIA Cloud Essentials+ (CLO-002) Cert Guide