Vendor: CompTIA

Exam Code:CLO-002

Exam Name: CompTIA Cloud Essentials+

Version: Demo

QUESTION 1

Which of the following allows for the management of network policies from a central portal while maintaining a hardware-agnostic approach?

A. Virtual private network

B. Software-defined network

C. Load balancing

D. Direct Connect

Correct Answer: B

Explanation: A software-defined network (SDN) is a network architecture that allows for the management of network policies from a central portal while maintaining a hardware- agnostic approach. SDN separates the control plane, which is responsible for making decisions about how to route traffic, from the data plane, which is responsible for forwarding traffic based on the control plane\\'s instructions. SDN enables network administrators to configure, monitor, and manage network devices and services using a software application, regardless of the vendor or type of hardware. SDN also provides automation, programmability, scalability, and flexibility for network operations. A virtual private network (VPN) is a network technology that creates a secure and encrypted connection over a public network, such as the Internet. A VPN allows remote users to access a private network and its resources securely. A VPN is not related to the management of network policies from a central portal or the hardware-agnostic approach of SDN. Load balancing is a network technique that distributes traffic across multiple servers or devices to optimize performance, reliability, and availability. Load balancing can be implemented using hardware or software, but it does not provide the same level of centralized management and control as SDN. Direct Connect is a service offered by some cloud providers that allows customers to establish a dedicated network connection between their on-premises network and the cloud provider\\'s network. Direct Connect bypasses the public Internet and provides lower latency, higher bandwidth, and more consistent network performance. However, Direct Connect is not a generic network architecture that supports a hardware-agnostic approach, and it does not offer the same degree of network programmability and automation as SDN. References: CompTIA Cloud Essentials+ CLO- 002 Study Guide, Chapter 4: Cloud Design Principles, Section 4.2: Cloud Network Concepts, Page 1051 and What is software-defined networking (SDN)? | Cloudflare

---

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 should be considered to ensure the availability of data that is accessed across multiple sites? (Choose two.)

A. Auto-scaling

B. Geo-redundancy

C. Backup

D. Provisioning

E. Locality

F. Zones

Correct Answer: BC

Explanation: Geo-redundancy and backup are two methods that can ensure the availability of data that is accessed across multiple sites. Geo-redundancy is the practice of storing data in more than one geographic location, such as different regions, countries, or continents. This can improve the data availability by reducing the impact of natural disasters, network failures, or malicious attacks that may affect one site. Geo-redundancy can also improve the data performance by allowing users to access the data from the nearest or fastest site. Backup is the process of creating and storing copies of data that can be used to restore the original data in case of data loss, corruption, or deletion. Backup can ensure the data availability by providing a way to recover the data from a previous state, such as before a hardware failure, software error, or human error. Backup can also protect the data from accidental or intentional modifications that may compromise its integrity or security. Geo-redundancy and backup are different from other options, such as auto-scaling, provisioning, locality, and zones. Auto-scaling is the ability of a cloud service to automatically adjust the amount of resources allocated to a workload based on the demand or usage. Provisioning is the process of allocating and configuring the resources needed to run a cloud service or application. Locality is the principle of storing data close to where it is used, such as in the same region, country, or jurisdiction. Zones are logical or physical subdivisions of a cloud region that provide isolation and redundancy for the cloud resources. While these options may also affect the data availability, they do not directly address the data access across multiple sites, which is the focus of the question.

References: Extending a Datastore Across Two Sites with Stretched Clusters, SQL Server Multi-Subnet Clustering - SQL Server Always On, What Is a Distributed Database? {Features, Benefits and Drawbacks}, Cloud Computing Availability - CompTIA Cloud Essentials+ (CLO-002) Cert Guide

---

QUESTION 4

Which of the following techniques helps an organization determine benchmarks for application performance within a set of resources?

A. Auto-scaling

B. Load testing

C. Sandboxing

D. Regression testing

Correct Answer: B

Explanation: Load testing is the technique that helps an organization determine benchmarks for application performance within a set of resources. Load testing is the process of simulating a high volume of user requests or traffic to a cloud application or service, and measuring its response time, throughput, availability, and reliability. Load testing can help an organization to evaluate the performance and scalability of the cloud application or service, as well as to identify and resolve any bottlenecks, errors, or failures. Load testing can also help the organization to optimize the resource utilization and allocation, and to plan for future growth or peak demand. Load testing can be done using various tools, such as JMeter, LoadRunner, or BlazeMeter12 References: CompTIA Cloud Essentials+ Certification Exam Objectives3, CompTIA Cloud Essentials+ Study Guide, Chapter 6: Cloud Connectivity and Load Balancing4, Cloud Essentials+ Certification Training2

QUESTION 5

A company is required to move its human resources application to the cloud to reduce capital expenses. The IT team does a feasibility analysis and learns the application requires legacy infrastructure and cannot be moved to the cloud.

Which of the following is the MOST appropriate cloud migration approach for the company?

A. Lift and shift

B. Hybrid

C. Rip and replace

D. In-place upgrade

Correct Answer: B

A hybrid cloud migration approach involves using a combination of on-premises and cloud resources to host an application. A hybrid cloud migration approach is suitable for applications that have dependencies or requirements that cannot be met by the cloud alone, such as legacy infrastructure, compliance, security, or performance1. A hybrid cloud migration approach can help reduce capital expenses by moving some components of the application to the cloud, while retaining others on-premises. A hybrid cloud migration approach can also provide flexibility, scalability, and resilience to the application, as it can leverage the best features of both environments2. A lift and shift cloud migration approach involves moving an application to the cloud as-is, without making any significant changes to its architecture or

configuration. A lift and shift cloud migration approach is not appropriate for applications that require legacy infrastructure and cannot be moved to the cloud, as it would result in compatibility issues, performance degradation, or increased costs3. A rip and replace cloud migration approach involves discarding an application and replacing it with a new one that is designed for the cloud. A rip and replace cloud migration approach is not appropriate for applications that require legacy infrastructure and cannot be moved to the cloud, as it would result in loss of functionality, data, or customization, as well as increased complexity, risk, and cost4. An in-place upgrade cloud migration approach involves updating an application to a newer version that is compatible with the cloud, without changing its location or platform. An in- place upgrade cloud migration approach is not appropriate for applications that require legacy infrastructure and cannot be moved to the cloud, as it would not reduce capital expenses or provide any benefits of the cloud. References: CompTIA Cloud Essentials+ CLO-002 Study Guide, Chapter 2: Cloud Migration, pages 49-50.

QUESTION 6

A company is discontinuing its use of a cloud provider. Which of the following should the provider do to ensure there is no sensitive data stored in the company\\'s cloud?

A. Replicate the data.

B. Encrypt the data.

C. Lock in the data.

D. Sanitize the data.

Correct Answer: D

Explanation: Data sanitization is the process of deliberately, permanently, and irreversibly removing or destroying the data stored on a memory device. Data sanitization is a security best practice and often a compliance requirement for sensitive or confidential data. Data sanitization ensures that the data cannot be recovered by any means, even by advanced forensic tools. Data sanitization can be done by overwriting, degaussing, or physically destroying the storage media. When a company discontinues its use of a cloud provider, the provider should sanitize the data to prevent any unauthorized access, leakage, or breach of the company\\'s data. References: CompTIA Cloud Essentials+ Certification Exam Objectives1, CompTIA Cloud Essentials+ Study Guide, Chapter 4: Cloud Storage2, Data sanitization for cloud storage3

QUESTION 7

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 8

Following a risk assessment, a company decides to adopt a multicloud strategy for its IT applications. Which of the following is the company trying to avoid as part of its risk mitigation strategy?

A. Geo-redundancy

B. Vendor lock-in

C. High availability

D. Data sovereignty

Correct Answer: D

Explanation: A company that adopts a multicloud strategy for its IT applications is trying to avoid vendor lock-in as part of its risk mitigation strategy. Vendor lock-in is a situation where the customer becomes dependent on a single cloud provider and faces high switching costs and technical challenges if they want to migrate to another provider. Vendor lock-in can limit the customer\\'s flexibility, choice, and control over their IT resources and expose them to the risks of service degradation, price increases, or vendor lockout12. A multicloud strategy is an approach that uses multiple cloud providers for different IT applications, based on the best fit for each workload. A multicloud strategy can help the customer avoid vendor lock-in by reducing their reliance on any single provider, increasing their bargaining power, and enabling them to leverage the best features and services from different providers34. References: CompTIA Cloud Essentials+ CLO-002 Study Guide, Chapter 2: Cloud Concepts and Models, Section 2.4: Cloud Service Challenges, p. 76-771 What is vendor lock-in? | Vendor lock-in and cloud computing 2 Avoiding vendor lock-in with the help of multicloud 3 How to Avoid Vendor Lock-In with Cloud Computing - Seagate 4

QUESTION 9

Which of the following activities in a cloud environment requires a defined scope and formal authorization from the CSP?

A. Orchestration

B. Penetration testing

C. Sandboxing

D. Vulnerability scanning

Correct Answer: B

Explanation: Penetration testing, also known as ethical hacking, is a security assessment methodology that involves simulating a cyberattack on a cloud-based system or service to identify and exploit vulnerabilities and weaknesses.

Penetration testing can help to evaluate the security posture of a cloud environment and provide recommendations for improvement12

Penetration testing in a cloud environment requires a defined scope and formal authorization from the cloud service provider (CSP), because it can have significant impacts on the cloud infrastructure, applications, and data. Penetration

testing can potentially cause damage, disruption, or breach of the cloud resources, as well as violate the terms of service or the service level agreements of the CSP. Therefore, before conducting penetration testing in a cloud environment,

the customer must obtain the consent and approval of the CSP, and follow the guidelines and policies of the CSP regarding the scope, duration, frequency, and methods of the testing3 Orchestration, sandboxing, and vulnerability scanning

are not activities that require a defined scope and formal authorization from the CSP, because they are less intrusive and disruptive than penetration testing. Orchestration is the process of automating and coordinating the deployment and

management of cloud resources using tools and scripts. Sandboxing is the process of creating and isolating a testing environment within the cloud to experiment with new features or applications without affecting the production environment.

Vulnerability scanning is the process of detecting and reporting the known vulnerabilities and misconfigurations in the cloud resources using automated tools. These activities can help to improve the efficiency, flexibility, and security of the

cloud environment, but they do not involve actively exploiting or compromising the cloud resources. Therefore, they do not require the same level of permission and oversight from the CSP as penetration testing.

References: 1: https://www.eccouncil.org/cybersecurity-exchange/penetration- testing/cloud-penetration-testing/, 1 2: https://www.comptia.org/training/books/cloud- essentials-clo-002-study-guide, page 48 3: https://www.browserstack.com/

guide/cloud- penetration-testing, 2 : https://www.prplbx.com/resources/blog/cloud-pentesting/, 3 :

https://www.comptia.org/training/books/cloud-essentials-clo-002-study-guide, page 46 :

https://www.comptia.org/training/books/cloud-essentials-clo-002-study-guide, page 44 :

https://www.comptia.org/training/books/cloud-essentials-clo-002-study-guide, page 48

QUESTION 10

Which of the following is the cloud storage technology that would allow a company with 12 nearly identical servers to have the SMALLEST storage footprint?

A. Capacity on demand

B. Compression

C. Software-defined storage

D. Deduplication

Correct Answer: D

Explanation: Deduplication is the cloud storage technology that would allow a company with 12 nearly identical servers to have the smallest storage footprint. Deduplication is the process of eliminating redundant or duplicate data blocks within a storage system, and replacing them with pointers to a single copy of the data. Deduplication can reduce the amount of storage space required, as well as the bandwidth and cost of data transfer. Deduplication is especially effective for data that has a high degree of similarity, such as backup data, virtual machine images, or server data. Deduplication can be performed at the source or the target, and at the file or the block level. References: CompTIA Cloud Essentials+ Certification Exam Objectives1, CompTIA Cloud Essentials+ Study Guide, Chapter 4: Cloud Storage2, Data Deduplication in Cloud Computing3

QUESTION 11

Which of the following risks is MOST likely to be accepted as a result of transferring business to a single CSP?

A. Vendor lock-in

B. The inability to scale

C. Data breach due to a break-in

D. Loss of equipment due to a natural disaster

Correct Answer: A

Explanation: Vendor lock-in is a situation where a customer becomes dependent on a single cloud service provider (CSP) and cannot easily switch to another vendor without substantial cost, technical incompatibility, or legal constraints1. Vendor lock-in is a risk that is most likely to be accepted as a result of transferring business to a single CSP, because it may offer some benefits such as lower prices, higher performance, or better integration. However, vendor lock-in also has some drawbacks, such as reduced flexibility, increased dependency, and limited innovation2. Therefore, customers should carefully weigh the pros and cons of vendor lock-in before choosing a CSP and try to avoid or mitigate it by using open standards, multi-cloud strategies, or contractual agreements3. References: What is vendor lock-in? | Vendor lock-in and cloud computing; What Is Cloud Vendor Lock-In (And How To Break Free)? - CAST AI; CompTIA Cloud Essentials

+ CLO- 002 Study Guide, Chapter 3: Cloud Computing Concepts, page 97.

QUESTION 12

A business analysis team is reviewing a report to try to determine the costs for a cloud application. The report does not allow separating costs by application.

Which of the following should the team use to BEST report on the costs of the specific cloud application?

A. Right-sizing

B. Content management

C. Optimization

D. Resource tagging

Correct Answer: D

Explanation: Resource tagging is a method of assigning metadata to cloud resources, such as instances, volumes, buckets, databases, etc. Resource tagging can help identify, organize, and manage cloud resources based on various criteria,

such as name, purpose, owner, environment, or cost center1. Resource tagging can also help track and report the costs of cloud resources, as the cloud service provider can generate billing and cost management reports based on the tags

applied to the resources2. Resource tagging is the best option for the business analysis team to report on the costs of the specific cloud application, as it would enable them to separate and filter the costs by the application tag. Right-sizing is

a technique of adjusting the size and type of cloud resources to match the actual needs and usage patterns of an application3. Right-sizing can help optimize the performance and cost of cloud resources, but it does not directly help report on

the costs of the specific cloud application, as it does not provide a way to separate and filter the costs by the application.

Content management is a process of creating, storing, organizing, and delivering digital content, such as documents, images, videos, etc. Content management can help manage the lifecycle and accessibility of digital content, but it does not

directly help report on the costs of the specific cloud application, as it does not provide a way to separate and filter the costs by the application.

Optimization is a process of improving the efficiency and effectiveness of cloud resources, such as by reducing waste, increasing performance, or enhancing security4. Optimization can help improve the quality and value of cloud resources,

but it does not directly help report on the costs of the specific cloud application, as it does not provide a way to separate and filter the costs by the application. References: CompTIA Cloud Essentials+ CLO-002 Study Guide, Chapter 5: Cloud

Resource Management, pages 187-188.