CLO-002$^{Q\&As}$

CompTIA Cloud Essentials+

Pass CompTIA CLO-002 Exam with 100% Guarantee

QUESTION 1

An IT company is planning to migrate its current infrastructure to the cloud due to support no longer being available and dependence on some legacy databases. Which of the following would be the BEST migration approach?

A. Rip and replace

B. Phased

C. Hybrid

D. Lift and shift

Correct Answer: D

Explanation: Lift and shift is a cloud migration approach that involves moving applications to the cloud as-is, without making any major changes to the application code or architecture. This approach is suitable for legacy applications that depend on specific databases or platforms that are no longer supported or available on-premise. Lift and shift can help reduce the cost and complexity of migration, while preserving the functionality and performance of the applications. However, lift and shift may not take full advantage of the cloud features and benefits, such as scalability, elasticity, and automation. Therefore, some applications may require further optimization or refactoring after the initial migration.

QUESTION 2

Which of the following models provides the SMALLEST amount of technical overhead?

A. SaaS

B. PaaS

C. MaaS

D. IaaS

Correct Answer: A

Explanation: SaaS, or software as a service, is a cloud computing model that provides on-demand access to ready-to-use, cloud-hosted application software. SaaS customers do not need to install, configure, manage, or maintain any hardware or software infrastructure to use the applications. The cloud service provider is responsible for all the technical aspects of the service, such as hosting, security, performance, availability, updates, and backups. SaaS customers only need an internet connection and a web browser or a mobile app to access the applications. SaaS provides the smallest amount of technical overhead for customers, as they do not have to deal with any of the underlying infrastructure or platform components. SaaS customers can focus on using the applications for their business needs, without worrying about the technical details. Some examples of SaaS applications are Gmail, Google Docs, Salesforce, Slack, and Zoom . References: : IaaS vs. PaaS vs. SaaS | IBM : Cloud Service Models Explained: SaaS, IaaS, PaaS, FaaS - Jelvix

QUESTION 3

A company is moving its long-term archive data to the cloud. Which of the following storage types will the company MOST likely use?

A. File

B. Object

C. Tape

D. Block

Correct Answer: B

Explanation: Object storage is a type of cloud storage that stores data as discrete units called objects. Each object has a unique identifier, metadata, and data. Object storage is ideal for storing long-term archive data in the cloud because it offers high scalability, durability, availability, and cost-effectiveness12. Object storage can handle large amounts of unstructured data, such as documents, images, videos, and backups, and allows users to access them from anywhere using a simple web interface3. Object storage also supports features such as encryption, versioning, lifecycle management, and replication to ensure the security and integrity of the archive data45. References: [CompTIA Cloud Essentials+ Certification Study Guide, Second Edition (LO-002)], Chapter 2: Cloud Computing Concepts, pages 36-37.

QUESTION 4

Which of the following is used to connect on-premises resources to resources located in a cloud environment?

A. Virtual private network

B. Access control list

C. Secure file transfer protocol

D. Software-defined network

Correct Answer: A

Explanation: A virtual private network (VPN) is a technology that creates a secure and encrypted connection over a public network, such as the internet, between two or more endpoints1. A VPN can be used to connect on-premises resources to resources located in a cloud environment, such as a virtual private cloud (VPC), which is a private network hosted within a public cloud2. A VPN allows the on-premises and cloud resources to communicate with each other as if they were on the same local network, without exposing the traffic to the public internet. A VPN can help to ensure the privacy, security, and reliability of the data and applications that are transferred between the on-premises and cloud environments3. A VPN is different from the other options listed in the question, which are not directly related to connecting on-premises resources to resources located in a cloud environment. An access control list (ACL) is a list of rules that defines who or what can access a specific resource, such as a file, a folder, a network, or a service. An ACL can help to enforce the security and authorization policies of the resource owner, but it does not create a secure connection between the on-premises and cloud environments. A secure file transfer protocol (SFTP) is a protocol that uses Secure Shell (SSH) to securely transfer files over a network. SFTP can help to protect the files from unauthorized access, modification, or interception, but it does not create a secure connection between the on-premises and cloud environments. A software-defined network (SDN) is a network architecture that decouples the network control and data planes, and allows the network to be programmatically configured and managed by software applications. SDN can help to improve the flexibility, scalability, and performance of the network, but it does not create a secure connection between the on-premises and cloud environments. References: What is a VPN? | How VPNs Work and Why You Need One | AVG, What is a VPN? What is a virtual private cloud (VPC)? - Cloudflare, What is a virtual private cloud (VPC)? What is a VPN and why is it important for cloud computing? | IBM, What is a VPN and why is it important for cloud computing? [What is an Access Control List (ACL)? - Definition from Techopedia], Access Control List (ACL) Definition. [What is SFTP? | How SFTP Works | Cloudflare], What is SFTP? [What is Software-Defined Networking (SDN)? | Cisco], Software-defined networking (SDN).

QUESTION 5

Which of the following would be expected from a security consultant who has been hired to investigate a data breach of a private cloud instance?

A. Incident report

B. Application scan results

C. Request for information

D. Risk register

Correct Answer: A

Explanation: An incident report is a document that summarizes the details of a security breach, such as the cause, impact, response, and lessons learned. It is expected from a security consultant who has been hired to investigate a data breach of a private cloud instance, as it provides a clear and concise account of what happened and how to prevent or mitigate future incidents. An incident report is also useful for communicating with stakeholders, regulators, customers, and other parties who may be affected by the breach. Application scan results are the output of a tool that scans an application for vulnerabilities, such as SQL injection, cross-site scripting, or broken authentication. They are not expected from a security consultant who has been hired to investigate a data breach of a private cloud instance, as they are more relevant for the development and testing phases of the application lifecycle. Application scan results may help identify potential weaknesses in the application, but they do not provide a comprehensive analysis of the breach. A request for information is a document that solicits information from vendors or service providers, such as their capabilities, pricing, or references. It is not expected from a security consultant who has been hired to investigate a data breach of a private cloud instance, as it is more relevant for the procurement and evaluation phases of the cloud service lifecycle. A request for information may help compare different cloud service options, but it does not provide a detailed report of the breach. A risk register is a document that records the risks associated with a project or an organization, such as their likelihood, impact, mitigation strategies, and status. It is not expected from a security consultant who has been hired to investigate a data breach of a private cloud instance, as it is more relevant for the risk management and governance phases of the cloud service lifecycle. A risk register may help identify and prioritize the risks that need to be addressed, but it does not provide a specific report of the breach. References: CompTIA Cloud Essentials+ CLO-002 Study Guide, Chapter 5: Security in the Cloud, Section 5.3: Incident Response, page 196 CompTIA Cloud Essentials+ CLO-002 Study Guide, Chapter 4: Cloud Service Management, Section 4.1: Cloud Service Lifecycle, page 145 CompTIA Cloud Essentials+ CLO-002 Study Guide, Chapter 2: Cloud Concepts, Section 2.4: Cloud Service Models, page 63

QUESTION 6

Which of the following describes the process of moving an application from an isolated data center to reduce latency and ensure close proximity to end users?

A. Replication

B. Zones

C. Geo-redundancy

D. Backup

Correct Answer: C

Explanation: Geo-redundancy is the distribution of mission-critical components or infrastructures, such as servers, across multiple data centers that reside in different geographic locations1. Geo-redundancy acts as a safety net in case the primary site fails or in the event of a disaster or an outage that impacts an entire region1. Geo-redundancy also reduces latency and ensures close proximity to end users by delivering web content from the nearest data center2. Geo-redundancy is a common feature of cloud computing, as it provides high availability, reliability, and performance for cloud applications and services2. Replication is the process of copying data from one location to another, such as from a primary site to a secondary site, or from one cloud provider to another3. Replication is a necessary but not sufficient condition for geo-redundancy, as it does not guarantee that the replicated data is accessible or consistent across different regions3. Replication can also introduce operational complexity and data synchronization issues3. Zones are logical or physical partitions of a cloud provider\\'s infrastructure that offer high availability and fault tolerance within a region4. Zones are usually located in the same or nearby data centers, and are connected by low-latency network links4. Zones can help distribute the workload and prevent single points of failure, but they do not provide geo-redundancy, as they are still vulnerable to regional outages or disasters4. Backup is the process of creating and storing copies of data for the purpose of recovery in case of data loss or corruption5. Backup is an important part of data protection and disaster recovery, but it does not provide geo-redundancy, as it does not ensure that the backup data is available or up-to-date in different regions5. Backup can also have longer recovery time and higher cost than geo-redundancy5. References: Use georedundancy to design highly available applications; Geo Redundancy Explained | Cloudify; Georedundancy - Open Telekom Cloud; Why geo-redundancy for cloud infrastructure is a `must have\\'; Geo-Redundancy: Why Is It So Important? | Unitrends.

QUESTION 7

A vendor stipulates it will provide incident response within two hours of a severity level A incident. Which of the following does this describe?

A. Maintenance agreement

B. Managed service agreement

C. Operating level agreement

D. Service level agreement

Correct Answer: D

Explanation: A service level agreement (SLA) is a contract between a service provider and a customer that defines the expected level of service, performance, availability, and quality of the service, as well as the responsibilities, obligations, and penalties of both parties. An SLA typically includes metrics and indicators to measure and monitor the service, such as response time, uptime, throughput, etc. An SLA also specifies the severity levels of incidents and the corresponding resolution times, such as two hours for a severity level A incident, which is the most critical and urgent. An SLA is different from a maintenance agreement, which is a contract that covers the repair and upkeep of equipment or software; a managed service agreement, which is a contract that covers the outsourcing of certain IT functions or processes to a third-party provider; or an operating level agreement, which is an internal agreement between different departments or units within an organization that support the delivery of a service. References: CompTIA Cloud Essentials+ Certification Exam Objectives1, CompTIA Cloud Essentials+ Study Guide, Chapter 2: Business Principles of Cloud Environments2, Service Level Agreements for Managed Services3

QUESTION 8

Which of the following concepts will help lower the attack surface after unauthorized user- level access?

A. Hardening

B. Validation

C. Sanitization

D. Audit

Correct Answer: A

Explanation: Hardening is the concept that will help lower the attack surface after unauthorized user-level access. Hardening is the process of securing a system by reducing its vulnerability to attacks. Hardening involves applying patches, updates, and configuration changes to eliminate or mitigate known weaknesses. Hardening also involves disabling or removing unnecessary services, features, and accounts that could be exploited by attackers. Hardening can help lower the attack surface by reducing the amount of code running, the number of entry points available, and the potential damage that can be caused by unauthorized access. References: CompTIA Cloud Essentials+ CLO-002 Study Guide, Chapter 4: Cloud Security, Section 4.2: Cloud Security Concepts, Page 153.

QUESTION 9

Which of the following testing techniques provides the BEST isolation for security threats?

A. Load

B. Regression

C. Black box

D. Sandboxing

Correct Answer: D

Explanation: Sandboxing is a testing technique that provides the best isolation for security threats. Sandboxing is a technique that creates a virtual environment that mimics the real system or application, but isolates it from the rest of the network. Sandboxing allows testers to run potentially malicious code or inputs without affecting the actual system or application, or exposing it to external attacks. Sandboxing can help testers to identify and analyze security threats, such as malware, ransomware, or zero-day exploits, without risking the integrity or availability of the real system or application. Sandboxing can also help testers to evaluate the effectiveness of security controls, such as antivirus, firewall, or encryption, in preventing or mitigating security threats. References: CompTIA Cloud Essentials+ CLO- 002 Study Guide, Chapter 3: Cloud Service Operations, Section 3.5: Testing and Development in the Cloud, Page 125. What is Sandboxing? Definition, Types, Benefits, and Best Practices - Spiceworks1

QUESTION 10

A company wants to deploy an application in a public cloud. Which of the following service models gives the MOST responsibility to the provider?

A. PaaS

B. IaaS

C. BPaaS

D. SaaS

Correct Answer: D

Explanation: SaaS stands for Software as a Service, which is a cloud service model that gives the most responsibility to the provider. In SaaS, the provider delivers the entire software application to the customer over the internet, without requiring any installation, configuration, or maintenance on the customer\\'s side. The customer only needs a web browser or a thin client to access the software, which is hosted and managed by the provider. The provider is responsible for the security, availability, performance, and updates of the software, as well as the underlying infrastructure, platform, and middleware. The customer has no control over the software, except for some limited customization and configuration options. The customer pays for the software usage, usually on a subscription or pay-per-use basis. SaaS is different from other service models, such as PaaS, IaaS, or BPaaS. PaaS stands for Platform as a Service, which is a cloud service model that provides the customer with a platform to develop, run, and manage applications without worrying about the infrastructure. The provider is responsible for the infrastructure, operating system, middleware, and runtime environment, while the customer is responsible for the application code, data, and configuration. IaaS stands for Infrastructure as a Service, which is a cloud service model that provides the customer with the basic computing resources, such as servers, storage, network, and virtualization. The provider is responsible for the physical infrastructure, while the customer is responsible for the operating system, middleware, runtime, application, and data. BPaaS stands for Business Process as a Service, which is a cloud service model that provides the customer with a complete business process, such as payroll, accounting, or human resources. The provider is responsible for the software, platform, and infrastructure that support the business process, while the customer is responsible for the input and output of the process. References: Cloud Service Models - CompTIA Cloud Essentials+ (CLO-002) Cert Guide, What is SaaS? Software as a service explained | InfoWorld, What is SaaS? Software as a Service Explained - Salesforce.com, What is SaaS? Software as a Service Definition - AWS

QUESTION 11

An incident response team requires documentation for an email phishing campaign against a company\\'s email server. Which of the following is the BEST resource to use to start the investigation?

A. Audit and system logs

B. Change management procedures

C. Departmental policies

D. Standard operating procedures

Correct Answer: A

Explanation: Audit and system logs are the best resource to use to start the investigation of an email phishing campaign against a company\\'s email server. Audit and system logs are records of events and activities that occur on a system or a network, such as user login, file access, configuration changes, or network traffic. Audit and system logs can help an incident response team to identify the source, scope, and impact of the phishing attack, as well as to collect evidence, trace the attack steps, and determine the root cause. Audit and system logs can also help the incident response team to evaluate the security posture and controls of the email server, and to recommend remediation and mitigation actions12 References: CompTIA Cloud Essentials+ Certification Exam Objectives3, CompTIA Cloud Essentials+ Study Guide, Chapter 7: Cloud Security, Cloud Essentials+ Certification Trainin

QUESTION 12

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 13

Which of the following is the result of performing a physical-to-virtual migration of desktop workstations?

A. SaaS

B. IaaS

C. VDI

D. VPN

Correct Answer: C

Explanation: VDI, or Virtual Desktop Infrastructure, is the result of performing a physical- to-virtual migration of desktop workstations. VDI is a technology that allows users to access and run desktop operating systems and applications from a centralized server in a data center or a cloud, instead of from a physical machine on their premises. VDI provides users with virtual desktops that are delivered over a network to various devices, such as laptops, tablets, or thin clients1. VDI offers several benefits, such as improved security, reduced costs, increased flexibility, and enhanced performance2. SaaS, or Software as a Service, is not the result of performing a physical-to-virtual migration of desktop workstations, but a cloud service model that provides ready-to-use software applications that run on the cloud provider\\'s infrastructure and are accessed via a web browser or an API3. SaaS does not involve migrating desktop workstations, but using software applications that are hosted and managed by the cloud provider. IaaS, or Infrastructure as a Service, is not the result of performing a physical-to-virtual migration of desktop workstations, but a cloud service model that provides access to basic computing resources, such as servers, storage, network, and virtualization, that are hosted on the cloud provider\\'s data centers and are rented on-demand. IaaS does not involve migrating desktop workstations, but renting infrastructure resources that can be used to host various workloads. VPN, or Virtual Private Network, is not the result of performing a physical-to-virtual migration of desktop workstations, but a technology that creates a secure and encrypted connection between a device and a network over the internet. VPN does not involve migrating desktop workstations, but connecting to a network that can provide access to remote resources or services. References: What is VDI? Virtual Desktop Infrastructure Definition - VMware; VDI Benefits: 7 Advantages

of Virtual Desktop Infrastructure; What is SaaS? Software as a service | Microsoft Azure; [What is IaaS? Infrastructure as a service | Microsoft Azure]; [What is a VPN? | HowStuffWorks].

QUESTION 14

A small business is engaged with a cloud provider to migrate from on-premises CRM software. The contract includes fixed costs associated with the product. Which of the following variable costs must be considered?

A. Time to market

B. Operating expenditure fees

C. BYOL costs

D. Human capital

Correct Answer: B

Explanation: Operating expenditure (OPEX) fees are variable costs that depend on the usage of cloud services, such as storage, bandwidth, compute, or licensing fees. OPEX fees are typically charged by the cloud provider on a monthly or pay-as-you-go basis. A small business that migrates from on-premises CRM software to a cloud provider must consider the OPEX fees as part of the total cost of ownership (TCO) of the cloud solution. OPEX fees can vary depending on the demand, performance, availability, and scalability of the cloud service. References: CompTIA Cloud Essentials+ Certification Exam Objectives1, CompTIA Cloud Essentials+ Study Guide, Chapter 2: Business Principles of Cloud Environments

QUESTION 15

Which of the following cloud principles will help manage the risk of a network breach?

A. Shared responsibility

B. Self-service

C. Availability

D. Elasticity

Correct Answer: A

Explanation: Shared responsibility is the cloud principle that states that the security and compliance of the cloud service are shared between the cloud service provider and the cloud customer. The cloud service provider is responsible for securing the cloud infrastructure, such as the hardware, software, networking, and facilities, while the cloud customer is responsible for securing the cloud data, applications, and access, such as the encryption, backup, authentication, and authorization. By following the shared responsibility principle, the cloud customer can manage the risk of a network breach by implementing appropriate security measures and controls on their end, such as firewalls, antivirus, VPNs, and IAM. The cloud customer can also leverage the security features and services offered by the cloud service provider, such as encryption, monitoring, auditing, and incident response. References: CompTIA Cloud Essentials+ CLO-002 Certification Study Guide, Chapter 5: Managing Cloud Security, Section 5.1: Understanding Cloud Security Concepts, Page 1611