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

A company is evaluating the capital expenditure necessary to modernize its on-premises datacenter. Management has directed that 50% of capital expenditure be reallocated to operating expenditure. Which of the following cloud characteristics applies?

A. BYOL

B. Billing chargeback

C. Pay-as-you-go

D. High availability

Correct Answer: C

Explanation: Pay-as-you-go is a cloud characteristic that applies to the scenario of reallocating capital expenditure to operating expenditure. Pay-as-you-go is a billing model in which customers only pay for the cloud resources and services they consume, without any upfront or fixed costs1. Pay-as-you-go allows customers to shift from CapEx to OpEx, as they do not need to invest in physical infrastructure or long-term contracts, but rather pay for what they use as they use it2. Pay-as-you-go also provides flexibility and scalability, as customers can adjust their usage and spending according to their needs and demand3. BYOL stands for Bring Your Own License, which is a cloud characteristic that allows customers to use their existing software licenses on the cloud provider\\'s platform, instead of purchasing new licenses from the cloud provider4. BYOL can help customers save money and avoid vendor lock-in, but it does not necessarily affect the allocation of CapEx and OpEx. Billing chargeback is a cloud characteristic that enables customers to allocate and track the costs of cloud resources and services to different departments, projects, or business units within their organization5. Billing chargeback can help customers optimize their cloud spending and improve accountability and transparency, but it does not directly influence the balance of CapEx and OpEx. High availability is a cloud characteristic that refers to the ability of a cloud system to remain operational and accessible at all times, even in the event of failures or disruptions. High availability is achieved by using redundant and fault-tolerant components, such as servers, networks, and storage, that can automatically failover or switch to backup resources in case of an outage. High availability is an important benefit of cloud computing, as it ensures reliability and performance, but it does not relate to the distinction between CapEx and OpEx. References:

1: CompTIA Cloud Essentials+ Certification Study Guide, Second Edition (LO-002), Chapter 2, page 37.

2: CompTIA Cloud Essentials+ Certification Study Guide, Second Edition (LO-002), Chapter 3, page 71.

3: CompTIA Cloud Essentials+ Certification Study Guide, Second Edition (LO-002), Chapter 3, page 72.

4: CompTIA Cloud Essentials+ Certification Study Guide, Second Edition (LO-002), Chapter 2, page 40.

5: CompTIA Cloud Essentials+ Certification Study Guide, Second Edition (LO-002), Chapter 3, page 78. [6]: CompTIA Cloud Essentials+ Certification Study Guide, Second Edition (LO-002), Chapter 2, page 35. [7]: CompTIA Cloud Essentials+ Certification Study Guide, Second Edition (LO-002), Chapter 4, page 99.

QUESTION 2

A company hired a DevOps engineer to move business systems to the cloud. The current systems administrator does not have scripting experience and has been deploying servers manually. Which of the following would BEST optimize this process?

A. Infrastructure as code deployment model

B. API integration to a cloud provider

C. Load testing

D. Continuous delivery/continuous integration

Correct Answer: A

Explanation: Infrastructure as code (IaC) is a key DevOps practice that involves the management of infrastructure, such as networks, compute services, databases, storages, and connection topology, in a descriptive model. IaC allows teams to develop and release changes faster and with greater confidence. IaC avoids manual configuration and enforces consistency by representing desired environment states via well-documented code in formats such as JSON. Infrastructure deployments with IaC are repeatable and prevent runtime issues caused by configuration drift or missing dependencies. IaC also helps teams to provision multiple test environments reliably on demand. Therefore, IaC would best optimize the process of moving business systems to the cloud and reduce the need for scripting experience and manual deployment. References: CompTIA Cloud Essentials+ CLO-002 Study Guide, Chapter 5: Cloud Migration, page 1971; What is infrastructure as code (IaC)? - Azure DevOps2

QUESTION 3

A DevOps team wants to document the upgrade steps for its public database solution. The team needs a dedicated virtual environment separate from the production systems to replicate multiple installations. Which of the following BEST represents what the team needs?

A. Containerization

B. Cold storage

C. Infrastructure as code

D. Sandboxing

Correct Answer: D

Explanation: According to the CompTIA Cloud Essentials objectives and documents, sandboxing is the best option for the DevOps team that wants to document the upgrade steps for its public database solution. Sandboxing is a technique that creates a virtual environment that is isolated from the production systems and allows the team to replicate multiple installations without affecting the real data or applications. Sandboxing is useful for testing, debugging, and experimenting with new features or configurations in a safe and controlled way. Sandboxing can also help the team to identify and resolve any potential issues or errors before deploying the upgrade to the production environment. The other options are not as suitable for the team\\'s needs. Containerization is a method of packaging software code with the necessary dependencies and libraries to run it on any platform or cloud. Containerization is beneficial for creating portable and scalable applications that can run consistently across different environments. However, containerization does not provide a dedicated virtual environment that is separate from the production systems, nor does it allow the team to replicate multiple installations of the same software. Cold storage is a type of data storage that is used for infrequently accessed or archived data. Cold storage is typically cheaper and slower than hot storage, which is used for frequently accessed or active data. Cold storage is not relevant for the team\\'s need to document the upgrade steps for its public database solution, as it does not involve data storage or access. Infrastructure as code is a practice of managing and provisioning cloud infrastructure using code or scripts, rather than manual processes or graphical user interfaces. Infrastructure as code is advantageous for automating and standardizing the deployment and configuration of cloud resources, such as servers, networks, or storage. However, infrastructure as code does not provide a dedicated virtual environment that is separate from the production systems, nor does it allow the team to replicate multiple installations of the same software. References: 1, 2, 3, 4

QUESTION 4

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 5

An architect recently discovered new opportunities the cloud can provide to the company. A business analyst is currently working with the architect to document the business use-case scenarios. Which of the following should be the architect\\'s NEXT step?

A. Initialize a PoC.

B. Conduct a feasibility study.

C. Perform a gap analysis.

D. Gather cloud requirements.

Correct Answer: B

Explanation: After documenting the business use-case scenarios, the architect\\'s next step should be to conduct a feasibility study. A feasibility study is an analysis of the viability and suitability of a proposed solution or project, such as migrating to the cloud. A feasibility study evaluates the technical, operational, financial, legal, and ethical aspects of the solution, as well as the risks and benefits involved. A feasibility study helps the architect to determine if the solution is feasible, desirable, and achievable, and to identify any potential issues or challenges that may arise1. A feasibility study

is one of the key components of a cloud assessment, which is a process of evaluating the readiness and suitability of an organization for cloud adoption1. A proof of concept (PoC) is a demonstration or prototype of a solution that shows how it works and what it can achieve. A PoC is usually done after a feasibility study, when the solution has been proven to be feasible and the requirements have been defined1. A gap analysis is a comparison of the current state and the desired state of a process, system, or organization. A gap analysis identifies the gaps or differences between the two states, and the actions or resources needed to close them. A gap analysis is usually done after a feasibility study and a PoC, when the solution has been validated and the goals have been established1. Gathering cloud requirements is the process of collecting and analyzing the needs and expectations of the stakeholders for the cloud solution. Gathering cloud requirements is usually done after a feasibility study and before a PoC, when the solution has been confirmed to be feasible and the scope has been defined1. References: CompTIA Cloud Essentials+ Certification | CompTIA IT Certifications, The New CompTIA Cloud Essentials+: Setting the Foundation For Vendor-specific IT Certifications, CompTIA Cloud Essentials CLO-002 Certification Study Guide

QUESTION 6

Which of the following are the appropriate responses to risks?

A. Mitigate, accept, avoid, validate

B. Migrate, accept, avoid, transfer

C. Mitigate, accept, avoid, transfer

D. Migrate, accept, avoid, validate

Correct Answer: C

Explanation: According to the CompTIA Cloud Essentials+ CLO-002 Study Guide, there are four common risk response types: avoid, share or transfer, mitigate, and accept1. These are the appropriate responses to risks, depending on the risk type, assessment, and attitude. The other options are incorrect because they include terms that are not valid risk responses. For example, migrate is not a risk response, but a cloud deployment strategy. Validate is not a risk response, but a quality assurance technique. References: CompTIA Cloud Essentials+ CLO-002 Study Guide, Chapter 4: Cloud Security, Section 4.2: Cloud Security Concepts, Page 153.

QUESTION 7

A vendor wants to distribute a cloud management application in a format that can be used on both public and private clouds, but one that does not include an underlying OS that would require patching and management. Which of the following would BEST meet this need?

A. Containerization

B. Federation

C. Collaboration

D. Microservices

Correct Answer: A

Explanation: Containerization is a software deployment process that bundles an application\\'s code with all the files and libraries it needs to run on any infrastructure. Containerization does not include an underlying operating system that would require patching and management, as containers share the host operating system kernel and run in isolated user

spaces. Containerization allows applications to run consistently and portably on any platform or cloud, regardless of the differences in operating systems, hardware, or configurations. Containerization also enables faster and easier deployment, scalability, and fault tolerance of applications. Therefore, containerization would best meet the need of a vendor who wants to distribute a cloud management application in a format that can be used on both public and private clouds. The other options are not relevant to the question. Federation is a process of integrating multiple cloud services or providers to create a unified cloud environment. Collaboration is a process of working together on a shared project or goal using cloud-based tools and platforms. Microservices are a software architecture style that breaks down a complex application into smaller, independent, and loosely coupled services that communicate through APIs. Microservices can be implemented using containers, but they are not a software deployment format. Therefore, the correct answer is A. Containerization. References: What is Containerization? - Containerization Explained - AWS, Containerization Explained | IBM, Microservices and containerisation - what IT manager needs to know, Containerized Microservices - Xamarin | Microsoft Learn.

QUESTION 8

A systems administrator must select a CSP while considering system uptime and access to critical servers. Which of the following is the MOST important criterion when choosing the CSP?

A. Elasticity

B. Scalability

C. Availability

D. Serviceability

Correct Answer: D

Explanation: Encryption in transit is the process of protecting data from unauthorized access or modification while it is being transferred from one location to another, such as from an on-premises data center to a cloud service provider. Encryption in transit uses cryptographic techniques to scramble the data and make it unreadable to anyone who intercepts it, except for the intended recipient who has the key to decrypt it. Encryption in transit is one of the best approaches to optimize data security in an IaaS migration, as it reduces the risk of data breaches, tampering, or leakage during the data transfer. Encryption in transit can be implemented using various methods, such as Transport Layer Security (TLS), Secure Sockets Layer (SSL), Internet Protocol Security (IPsec), or Secure Shell (SSH). Encryption in transit is different from other options, such as reviewing the risk register, performing a vulnerability scan, or performing server hardening. Reviewing the risk register is the process of identifying, analyzing, and prioritizing the potential threats and impacts to the data and the cloud environment. Performing a vulnerability scan is the process of detecting and assessing the weaknesses or flaws in the data and the cloud infrastructure that could be exploited by attackers. Performing server hardening is the process of applying security measures and configurations to the cloud servers to reduce their attack surface and improve their resilience. While these options are also important for data security, they do not directly address the data protection during the migration process, which is the focus of the question. References: What is encryption in transit? - Definition from WhatIs.com, Data Encryption in Transit Guidelines - UC Berkeley Security, Cloud Computing Security - CompTIA Cloud Essentials+ (CLO-002) Cert Guide

QUESTION 9

The Chief Financial Officer for a company that operates a popular SaaS application has noticed compute costs from the CSP are extremely high but storage costs are relatively low. Which of the following does the company MOST likely operate?

A. An email application

B. A CDN service

C. A gaming application

D. Audio streaming service

Correct Answer: C

Explanation: A gaming application is a type of SaaS application that requires high compute resources to run the game logic, graphics, physics, and networking. Gaming applications also need to handle a large number of concurrent users and provide low latency and high performance. Therefore, the compute costs from the CSP would be extremely high for a gaming application. On the other hand, a gaming application does not need much storage space, as most of the game data is stored on the client side or in memory. Therefore, the storage costs from the CSP would be relatively low for a gaming application. The other options are not likely to have high compute costs and low storage costs. An email application, a CDN service, and an audio streaming service all need to store large amounts of data on the cloud, which would increase the storage costs. An email application and a CDN service do not need much compute power, as they mainly involve sending and receiving data. An audio streaming service may need some compute power to process and encode the audio files, but not as much as a gaming application. Therefore, the correct answer is C. A gaming application. References:

Cloud Computing for Gaming Applications, Cloud Computing for Online Games: A Survey, Cloud Gaming: A Green Solution to Massive Multiplayer Online Games.

QUESTION 10

A company wants to migrate mission-critical applications to the cloud. In order for technicians to build, decommission, and perform other routine functions, which of the following cloud characteristics would BEST satisfy this business requirement?

A. Self-service

B. Elasticity

C. Broad network access

D. Availability

Correct Answer: A

Explanation: Self-service is one of the five essential characteristics of cloud computing, along with broad network access, resource pooling, rapid elasticity, and measured service1. Self-service enables cloud customers to provision and

manage cloud resources without requiring human interaction from the cloud service provider2. Self-service allows cloud customers to have more control, flexibility, and agility over their cloud environment, and to perform various tasks such as

building, decommissioning, scaling, monitoring, and configuring cloud resources according to their business needs and preferences3. Self- service is the best cloud characteristic to satisfy the business requirement of migrating mission-critical

applications to the cloud, as it would enable technicians to perform routine functions more efficiently and effectively, and to respond to changing demands and situations more quickly and dynamically.

Broad network access is another essential characteristic of cloud computing, which means that cloud resources are

available over the network and can be accessed by diverse customer platforms, such as laptops, mobile phones, tablets,

etc1. Broad network access is an important feature of cloud computing, as it enables cloud customers to access their cloud resources anytime and anywhere, and to use different devices and methods to interact with the cloud. However,

broad network access is not the best cloud characteristic to satisfy the business requirement of migrating mission-critical applications to the cloud, as it does not directly relate to the ability of technicians to build, decommission, and perform

other routine functions on the cloud resources.

Elasticity is another essential characteristic of cloud computing, which means that cloud resources can be rapidly and dynamically scaled up or down according to the customer\\'s demand1. Elasticity is a key benefit of cloud computing, as it

enables cloud customers to optimize the utilization and performance of their cloud resources, and to pay only for what they use. However, elasticity is not the best cloud characteristic to satisfy the business requirement of migrating mission-

critical applications to the cloud, as it does not directly relate to the ability of technicians to build, decommission, and perform other routine functions on the cloud resources.

Availability is not one of the five essential characteristics of cloud computing, but rather a quality attribute or a non-functional requirement of cloud computing. Availability refers to the degree to which a system or service is operational and

accessible when required4. Availability is a critical factor for cloud computing, especially for mission-critical applications, as it affects the reliability and continuity of the cloud service. However, availability is not the best cloud characteristic to

satisfy the business requirement of migrating mission-critical applications to the cloud, as it does not directly relate to the ability of technicians to build, decommission, and perform other routine functions on the cloud resources.
References:

CompTIA Cloud Essentials+ CLO-002 Study Guide, Chapter 1:

Cloud Computing Concepts, pages 11-15.

QUESTION 11

A startup company wants to develop a new voice assistant that leverages technology that can improve its product based on end user input. Which of the following would MOST likely accomplish this goal?

A. Big Data

B. Blockchain

C. VDI

D. Machine learning

Correct Answer: D

Explanation: Machine learning is a technology that enables a voice assistant to improve its product based on end user input. Machine learning is a branch of artificial intelligence that allows systems to learn from data and experience, without being explicitly programmed. Machine learning can help a voice assistant to understand natural language,

recognize speech, generate responses, and adapt to user feedback. Machine learning can also help a voice assistant to personalize its service, by learning the preferences, habits, and needs of each user. Machine learning can make a voice assistant more intelligent, accurate, and user-friendly over time. References: CompTIA Cloud Essentials+ CLO-002 Study Guide, Chapter 2: Cloud Concepts, Section 2.2: Cloud Technologies, Page 55.

QUESTION 12

An analyst is reviewing a report on a company\\'s cloud resource usage. The analyst has noticed many of the cloud instances operate at a fraction of the full processing capacity. Which of the following actions should the analyst consider to

lower costs and improve efficiency?

A. Consolidating into fewer instances

B. Using spot instances

C. Right-sizing compute resource instances

D. Negotiating better prices on the company\\'s reserved instances

Correct Answer: C

Explanation: Right-sizing compute resource instances is the process of matching instance types and sizes to workload performance and capacity requirements at the lowest possible cost. It\\'s also the process of identifying opportunities to eliminate or downsize instances without compromising capacity or other requirements, which results in lower costs and higher efficiency1. Right-sizing is a key mechanism for optimizing cloud costs, but it is often ignored or delayed by organizations when they first move to the cloud. They lift and shift their environments and expect to right-size later. Speed and performance are often prioritized over cost, which results in oversized instances and a lot of wasted spend on unused resources2. Right-sizing compute resource instances is the best action that the analyst should consider to lower costs and improve efficiency, as it can help reduce the amount of resources and money spent on instances that operate at a fraction of the full processing capacity. Right- sizing can also improve the performance and reliability of the instances by ensuring that they have enough resources to meet the workload demands. Right-sizing is an ongoing process that requires continuous monitoring and analysis of the instance usage and performance metrics, as well as the use of tools and frameworks that can simplify and automate the right-sizing decisions1. Consolidating into fewer instances, using spot instances, or negotiating better prices on the company\\'s reserved instances are not the best actions that the analyst should consider to lower costs and improve efficiency, as they have some limitations and trade-offs compared to right-sizing. Consolidating into fewer instances can reduce the number of instances, but it does not necessarily optimize the type and size of the instances. Consolidating can also introduce performance and availability issues, such as increased latency, reduced redundancy, or single points of failure3. Using spot instances can reduce the cost of instances, but it also introduces the risk of interruption and termination, as spot instances are subject to fluctuating prices and availability based on the supply and demand of the cloud provider4. Negotiating better prices on the company\\'s reserved instances can reduce the cost of instances, but it also requires a long-term commitment and upfront payment, which reduces the flexibility and scalability of the cloud environment5. References: Right Sizing - Cloud Computing Services; The 6-Step Guide To Rightsizing Your Instances - CloudZero; Consolidating Cloud Services: How to Do It Right | CloudHealth by VMware; Spot Instances - Amazon Elastic Compute Cloud; Reserved Instances - Amazon Elastic Compute Cloud.

QUESTION 13

A contract that defines the quality and performance metrics that are agreeable to both parties is called an:

A. SOP.

B. SOA.

C. SOW.

D. SLA.

Correct Answer: D

Explanation: A service level agreement (SLA) is a contract that defines the quality and performance metrics that are agreeable to both parties. An SLA specifies the expectations and responsibilities of the service provider and the customer in terms of service availability, reliability, security, and responsiveness. An SLA also defines the penalties or remedies for non-compliance with the agreed-upon metrics. An SLA is a key component of cloud computing contracts, as it ensures that the cloud service provider delivers the service according to the customer\\'s requirements and expectations12. References: CompTIA Cloud Essentials+ CLO-002 Study Guide, Chapter 3: Cloud Business Principles, Section 3.4: Cloud Service Agreements, p. 117-1181 What is SLA? - Service Level Agreement Explained - AWS 2

QUESTION 14

Which of the following types of risk is MOST likely to be associated with moving all data to one cloud provider?

A. Vendor lock-in

B. Data portability

C. Network connectivity

D. Data sovereignty

Correct Answer: A

Explanation: Vendor lock-in is the type of risk that is most likely to be associated with moving all data to one cloud provider. Vendor lock-in refers to the situation where a customer is dependent on a particular vendor\\'s products and services to such an extent that switching to another vendor becomes difficult, time-consuming, or expensive. Vendor lock-in can limit the customer\\'s flexibility, choice, and control over their cloud environment, and expose them to potential issues such as price increases, service degradation, security breaches, or compliance violations. Vendor lock-in can also prevent the customer from taking advantage of new technologies, innovations, or opportunities offered by other vendors. Vendor lock-in can be caused by various factors, such as proprietary formats, standards, or protocols, lack of interoperability or compatibility, contractual obligations or penalties, or high switching costs12 References: CompTIA Cloud Essentials+ Certification Exam Objectives3, CompTIA Cloud Essentials+ Study Guide, Chapter 2: Business Principles of Cloud Environments2, Moving All Data to One Cloud Provider: Understanding Risks1

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