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.leads4pass.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

Which of the following security concerns is BEST addressed by moving systems to the cloud?

A. Availability

B. Authentication

C. Confidentiality

D. Integrity

Correct Answer: A

Explanation: Availability is the security concern that is best addressed by moving systems to the cloud. Availability refers to the ability of a system or service to be accessible and functional when needed by authorized users. Availability is one of the key benefits of cloud computing, as it provides high reliability, scalability, and performance for the cloud systems and services. Cloud providers use various techniques and technologies to ensure availability, such as: Redundancy: Cloud providers replicate the data and resources across multiple locations, such as regions, zones, or data centers, to prevent single points of failure and provide backup and failover capabilities in case of disasters or disruptions. Load balancing: Cloud providers distribute the workload and traffic among multiple servers or instances to optimize the resource utilization and performance of the cloud systems and services. Auto-scaling: Cloud providers automatically adjust the amount of resources allocated to the cloud systems and services based on the demand or usage, to prevent overloading or underutilizing the resources and ensure consistent availability. Monitoring and recovery: Cloud providers continuously monitor the health and status of the cloud systems and services, and provide alerts and notifications in case of any issues or incidents. Cloud providers also provide tools and methods to recover the cloud systems and services from failures or errors, such as snapshots, backups, or restore points. Availability is different from other security concerns, such as authentication, confidentiality, or integrity. Authentication is the process of verifying the identity and credentials of a user or system before granting access to the cloud systems and services. Confidentiality is the process of protecting the data and information from unauthorized access or disclosure, such as by using encryption, access control, or data masking. Integrity is the process of ensuring the data and information are accurate, complete, and consistent, and have not been modified or corrupted by unauthorized or malicious parties, such as by using hashing, digital signatures, or checksums. References: Cloud Computing Availability - CompTIA Cloud Essentials+ (CLO-002) Cert Guide, Cloud Security ?Amazon Web Services (AWS), Azure infrastructure availability - Azure security | Microsoft Learn, What is Cloud Security? Cloud Security Defined | IBM

QUESTION 2

Transferring all of a customer\\'s on-premises data and virtual machines to an appliance, and then shipping it to a cloud provider is a technique used in a:

A. phased migration approach.

B. replatforming migration approach.

C. rip and replace migration approach.

D. lift and shift migration approach.

Correct Answer: D

Explanation: A lift and shift migration approach, also known as rehosting, is a cloud migration strategy where applications and infrastructure are moved from one environment to another without making substantial changes to the

underlying architecture123. This approach can be faster, cheaper, and less risky than other migration strategies, as it does not require extensive redesign or reconfiguration of the applications. However, it may also limit the ability to leverage the native features and benefits of the cloud platform, such as scalability, elasticity, and performance1245. One of the challenges of a lift and shift migration is transferring large amounts of data and virtual machines over the network, which can be time-consuming, costly, and prone to errors. To overcome this challenge, some cloud providers offer a technique where the customer can transfer all of their on-premises data and virtual machines to an appliance, such as a physical storage device or a server, and then ship it to the cloud provider. The cloud provider then uploads the data and virtual machines to the cloud platform, where they can be accessed by the customer12. This technique can reduce the network bandwidth and latency issues, as well as the security risks, associated with transferring data over the internet. However, it may also introduce additional costs and delays for shipping and handling the appliance, as well as the risk of damage or loss during transit2. Therefore, transferring all of a customer\\'s on-premises data and virtual machines to an appliance, and then shipping it to a cloud provider is a technique used in a lift and shift migration approach. References:

1: Lift and Shift: An Essential Guide | IBM

2: What Is Lift and Shift? | 5 Strategies to Consider | NetApp

3: What Is Lift and Shift Migration? | Pure Storage

4: Lift and Shift: Business Benefits, Planning and Execution - NetApp

5: Lift and Shift Cloud Migration: Benefits, Disadvantages and Use Cases ...

QUESTION 3

An organization plans to keep three of its cloud servers online for another nine months and a fourth server online for a year. The current pricing is $200 per month per server. The cloud provider announced the sale price of $1,500 per year per reserved instance.

Which of the following represents the cost savings by converting all four of the cloud servers to reserved instances?

A. $900

B. $1,800

C. $2,400

D. $3,600

Correct Answer: B

Explanation: The cost savings by converting all four of the cloud servers to reserved instances can be calculated as follows:

The current pricing is $200 per month per server, which means the total cost for keeping three servers online for another nine months is $200 x 3 x 9 = $5,400, and the total cost for keeping one server online for a year is $200 x 1 x 12 =

$2,400. The total cost for all four servers is $5,400 + $2,400 = $7,800. The sale price of $1,500 per year per reserved instance means the total cost for converting all four servers to reserved instances is $1,500 x 4 = $6,000. The cost savings

by converting all four servers to reserved instances is $7,800 - $6,000 = $1,800.

References: CompTIA Cloud Essentials+ Certification Exam Objectives1, CompTIA Cloud Essentials+ Study Guide,

Chapter 2: Business Principles of Cloud Environments2, Cloud Essentials+ Certification Training3

QUESTION 4

A large enterprise has the following invoicing breakdown of current cloud consumption spend:

Department	Cost	Server
Marketing	$895 per month	Reserved AZ5
Accounting	$422 per month	Spot AZ5
IT operations	$485 per month	Spot AZ5

The level of resources consumed by each department is relatively similar. Which of the following is MOST likely affecting monthly costs?

A. The servers in use by the marketing department are in an availability zone that is generally expensive.

B. The servers in use by the accounting and IT operations departments are in different geographic zones with lower pricing.

C. The accounting and IT operations departments are choosing to bid on non-committed resources.

D. The marketing department likely stores large media files on its servers, leading to increased storage costs.

Correct Answer: D

Explanation: The marketing department likely stores large media files on its servers, leading to increased storage costs. This is because the marketing department is responsible for creating and distributing various types of digital content, such as videos, images, podcasts, and webinars, to promote the products and services of the enterprise. These media files tend to be large in size and require more storage space than other types of data, such as text documents or spreadsheets. Therefore, the marketing department consumes more storage resources than the other departments, which increases the monthly cloud costs for the enterprise. References: CompTIA Cloud Essentials+ CLO-002 Study Guide, Chapter 3: Cloud Service and Delivery Models, Section 3.2: Cloud Storage, Page 97

QUESTION 5

Which of the following describes the contractually allowed downtime for a cloud-hosted application?

A. SOW

B. SLA

C. SOP

D. SOA

Correct Answer: B

Explanation: An SLA (service level agreement) is a contract between a cloud service provider and a cloud customer that defines the expected level of service, performance, availability, and reliability of the cloud service. An SLA also specifies

the contractually allowed downtime for a cloud-hosted application, which is the maximum amount of time that the application can be unavailable or inaccessible without violating the SLA. The contractually allowed downtime is usually expressed as a percentage of uptime, such as 99.9% or 99.99%, which corresponds to a certain number of hours or minutes per year, month, week, or day. For example, an SLA with 99.9% uptime means that the cloud service can be down for up to 8.76 hours per year, or 43.8 minutes per month, or 10.1 minutes per week, or 1.44 minutes per day. If the cloud service provider fails to meet the SLA, the cloud customer may be entitled to compensation or other remedies, such as credits, refunds, or termination of the contract. References: CompTIA Cloud Essentials+ CLO-002 Certification Study Guide, page 27-28; CompTIA Cloud Essentials+ Certification Training, CertMaster Learn for Cloud Essentials+, Module 2: Business Principles of Cloud Environments, Lesson 2.4: Cloud Service Agreements, Topic 2.4.2: Service Level Agreements

QUESTION 6

Which of the following cloud deployment models has on-premises and off-site data?

A. Private

B. Community

C. Public

D. Hybrid

Correct Answer: D

Explanation: A hybrid cloud is a cloud deployment model that has on-premises and off-site data. A hybrid cloud is a combination of public and private clouds that are connected by a common network and share data and applications. A hybrid cloud allows an organization to leverage the benefits of both public and private clouds, such as scalability, cost-efficiency, security, and control. A hybrid cloud also enables an organization to move workloads and data between the clouds based on performance, availability, compliance, and cost requirements. For example, an organization can use a private cloud for sensitive data and applications, and a public cloud for less critical data and applications, or for temporary or seasonal workloads. A hybrid cloud can also provide backup and disaster recovery solutions by replicating data and applications between the clouds. References: CompTIA Cloud Essentials+ CLO-002 Study Guide, Chapter 2: Cloud Computing Concepts, page 511. Cloud Deployment Models: What\\'s the Difference? | VMware News and Stories2. What are the different types of cloud computing? | Google Cloud3. 5 Types of Cloud Deployment Models and How to Use Them

-MUO4.

QUESTION 7

Which of the following is a cloud service model that organizations use when their third-party ERP tool is provided as a complete service?

A. Public cloud

B. SaaS

C. Hybrid cloud

D. IaaS

Correct Answer: B

Explanation: SaaS, or software as a service, is a cloud service model that provides ready- to-use, cloud-hosted application software to customers. Customers do not need to install, manage, or maintain the software; they simply access it via an internet connection, usually through a web browser. SaaS applications are typically offered on a subscription or pay- per-use basis. Examples of SaaS applications include email, CRM, ERP, office productivity, and collaboration tools12. SaaS is different from the other cloud service models in terms of the level of abstraction and control. In SaaS, the cloud service provider manages everything from the underlying infrastructure to the application software, while the customer only controls the application settings and data. In contrast, in IaaS (infrastructure as a service), the customer has more control and responsibility over the servers, storage, networking, and operating systems, while the cloud service provider only manages the physical infrastructure. In PaaS (platform as a service), the customer has control and responsibility over the applications and data, while the cloud service provider manages the underlying infrastructure and the development tools and platforms12. Therefore, when an organization uses a third-party ERP tool as a complete service, it is using the SaaS cloud service model. The organization does not need to worry about the installation, configuration, or maintenance of the ERP software; it only needs to access it via the internet and pay for the usage. The cloud service provider takes care of the rest.

https://www.comptia.org/training/books/cloud-essentials-clo-002-study-guide https://www.amazon.com/CompTIA-Essentials-Certification-Second-CLO- 002/dp/1260461785

QUESTION 8

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 9

A new company directive requires all departments to ensure intellectual property is kept within a country\\'s borders. Which of the following concepts BEST represents this requirement?

A. Data portability

B. Data security

C. Data locality

D. Data sovereignty

Correct Answer: D

Explanation: Data sovereignty is the concept that best represents the requirement for keeping intellectual property within a country\\'s borders. Data sovereignty refers to the idea that data is subject to the laws and governance of the country in which it is stored or processed. Data sovereignty can have implications for data privacy, security, compliance, and access, as different countries may have different regulations, standards, or policies regarding data protection, ownership, or transfer. Data sovereignty can also affect the choice of cloud providers, as some cloud providers may store or process data in multiple locations across the world, which may not comply with the data sovereignty requirements of the customer or the country. Therefore, customers who need to ensure data sovereignty should carefully review the terms and conditions of the cloud provider, and choose the one that offers the appropriate data location, encryption, or isolation options12 References: CompTIA Cloud Essentials+ Certification Exam Objectives3, CompTIA Cloud Essentials+ Study Guide, Chapter 4: Cloud Storage2, Intellectual Property Localization1

QUESTION 10

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 11

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

QUESTION 12

A manufacturing company is selecting applications for a cloud migration. The company\\'s main concern relates to the ERP system, which needs to receive data from multiple industrial systems to generate the executive reports. Which of the following will provide the details needed for the company\\'s decision regarding the cloud migration?

A. Standard operating procedures

B. Feasibility studies

C. Statement of work

D. Benchmarks

Correct Answer: B

Explanation: Feasibility studies are the best option to provide the details needed for the company\\'s decision regarding the cloud migration. Feasibility studies are comprehensive assessments that evaluate the technical, financial, operational, and organizational aspects of moving an application or workload from one environment to another. Feasibility studies can help determine the suitability, viability, and benefits of migrating an application or workload to the cloud, as well as the challenges, risks, and costs involved. Feasibility studies can also help identify the best cloud solution and migration method for the application or workload, based on its requirements, dependencies, and characteristics. In the context of the manufacturing company, a feasibility study can help analyze the ERP system and its data sources, and provide information on how to migrate it to the cloud without compromising its functionality, performance, security, or compliance. A feasibility study can also help compare the cloud migration options with the current on-premises solution, and estimate the return on investment and the total cost of ownership of the cloud migration. Therefore, feasibility studies can provide the details needed for the company\\'s decision regarding the cloud migration. Standard operating procedures, statement of work, and benchmarks are not the best options to provide the details needed for the company\\'s decision regarding the cloud migration, as they have different purposes and scopes. Standard operating procedures are documents that describe the steps and tasks involved in performing a specific process or activity, such as installing, configuring, or troubleshooting an application or workload. Standard operating procedures can help ensure consistency, quality, and efficiency in the execution of a process or activity, but they do not provide information on the feasibility or suitability of migrating an application or workload to the cloud. Statement of work is a document that defines the scope, objectives, deliverables, and expectations of a project or contract, such as a cloud

migration project or contract. Statement of work can help establish the roles, responsibilities, and expectations of the parties involved in a project or contract, but it does not provide information on the feasibility or viability of migrating an application or workload to the cloud. Benchmarks are tests or measurements that evaluate the performance, quality, or reliability of an application or workload, such as the speed, throughput, or availability of an application or workload. Benchmarks can help compare the performance, quality, or reliability of an application or workload across different environments, such as on-premises or cloud, but they do not provide information on the feasibility or benefits of migrating an application or workload to the cloud. References: CompTIA Cloud Essentials+ CLO-002 Study Guide, Chapter 7: Cloud Migration, Section 7.1: Cloud Migration Concepts, Page 2031 and Navigating Success: The Crucial Role of Feasibility Studies in SAP Cloud Migration | SAP Blogs

QUESTION 13

A large online car retailer needs to leverage the public cloud to host photos that must be accessible from anywhere and available at anytime. Which of the following cloud storage types would be cost-effective and meet the requirements?

A. Cold storage

B. File storage

C. Block storage

D. Object storage

Correct Answer: D

Explanation: Object storage is a cloud storage type that would be cost-effective and meet the requirements of a large online car retailer that needs to host photos that must be accessible from anywhere and available at anytime. Object

storage is a type of cloud storage that stores data as objects, which consist of data, metadata, and a unique identifier. Object storage is ideal for storing large amounts of unstructured data, such as photos, videos, audio, documents, and web

pages. Object storage offers several advantages for the online car retailer, such as:

Cost-effectiveness: Object storage is typically cheaper than other types of cloud storage, such as file storage and block storage, because it does not require a complex file system or a high-performance storage network. Object storage also

offers pay-per-use pricing, which means the retailer only pays for the amount of storage they consume.

Accessibility: Object storage allows data to be accessed from anywhere and anytime, using a simple HTTP or HTTPS request. Object storage also supports RESTful APIs, which enable easy integration with web and mobile applications.

Object storage can also leverage content delivery networks (CDNs), which distribute data across multiple locations to improve performance and availability. Scalability: Object storage can scale to store virtually unlimited amounts of data,

without compromising performance or reliability. Object storage can also handle concurrent requests from multiple users, which is important for a high-traffic website like the online car retailer.

Durability: Object storage ensures data durability by replicating data across multiple servers or regions, which protects data from hardware failures, natural disasters, or human errors. Object storage also supports versioning, which allows

data to be restored to a previous state in case of accidental deletion or modification.

References: CompTIA Cloud Essentials+ CLO-002 Study Guide, Chapter 2: Cloud Concepts, Section 2.2: Cloud Technologies, Page 55. What Is Cloud Storage? Definition, Types, Benefits, and Best Practices - Spiceworks1 What Is

a Public

Cloud? | Google Cloud2

QUESTION 14

The cloud consumer compliance team requires the IT department to patch and update cloud resources properly. Which of the following cloud service delivery models will BEST suit this need?

A. SaaS

B. DBaaS

C. DRaaS

D. IaaS

Correct Answer: D

Explanation: Infrastructure as a service (IaaS) is a cloud service delivery model that provides on-demand infrastructure resources to organizations via the cloud, such as compute, storage, networking, and virtualization4. IaaS is the most suitable cloud service delivery model for patching and updating cloud resources properly, as it gives the cloud consumer compliance team more control and flexibility over the operating system, middleware, virtual machines, and any apps or data5. IaaS also enables automation and orchestration of the provisioning process, as well as scalability and reliability of the infrastructure6. References: IaaS vs PaaS vs SaaS vs DBaaS: Cloud Service Models Differences, The App Solutions PaaS vs IaaS vs SaaS: What\\'s the difference?, Google Cloud CompTIA Cloud Essentials CLO-002 Certification Study Guide, Chapter 1: Cloud Computing Concepts, page 23

QUESTION 15

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

CLO-002 Practice Test CLO-002 Study Guide CLO-002 Exam Questions